ID: 548854
Sample Name: ab.bin
Cookbook: default.jbs
Time: 16:46:45
Date: 06/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

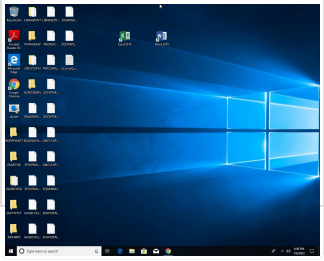
Windows Analysis Report ab.bin

Overview

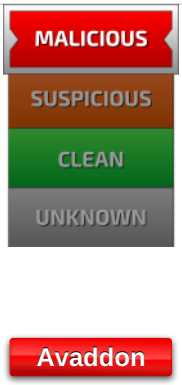
General Information

Sample Name:	ab.bin (renamed file extension from bin to exe)
Analysis ID:	548854
MD5:	0b486fe0503524c.
SHA1:	297dea71d48976..
SHA256:	1228d0f04f0ba82..
Infos:	

Most interesting Screenshot:



Detection

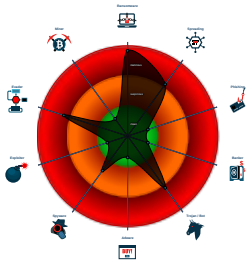


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Avaddon Ransomware
- Found ransom note / readme
- Antivirus / Scanner detection for sub…
- Yara detected RansomwareGeneric
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Sigma detected: Shadow Copies De…
- Sigma detected: Copying Sensitive …
- Yara detected PersistenceViaHidden…
- Spreads via windows shares (copies…
- Creates processes via WMI

Classification



Process Tree

- **System is w10x64**
- ab.exe (PID: 6212 cmdline: "C:\Users\user\Desktop\ab.exe" MD5: 0B486FE0503524CFE4726A4022FA6A68)
  - WMIC.exe (PID: 1744 cmdline: wmic SHADOWCOPY DELETE /nointeractive MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 7084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vssadmin.exe (PID: 5468 cmdline: vssadmin Delete Shadows /All /Quiet MD5: 7E30B94672107D3381A1D175CF18C147)
    - conhost.exe (PID: 7204 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WMIC.exe (PID: 7444 cmdline: wmic SHADOWCOPY DELETE /nointeractive MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 7496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vssadmin.exe (PID: 7608 cmdline: vssadmin Delete Shadows /All /Quiet MD5: 7E30B94672107D3381A1D175CF18C147)
    - conhost.exe (PID: 7616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WMIC.exe (PID: 7676 cmdline: wmic SHADOWCOPY DELETE /nointeractive MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 7684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vssadmin.exe (PID: 7752 cmdline: vssadmin Delete Shadows /All /Quiet MD5: 7E30B94672107D3381A1D175CF18C147)
    - conhost.exe (PID: 7788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ab.exe (PID: 4876 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe MD5: 0B486FE0503524CFE4726A4022FA6A68)
- WMIC.exe (PID: 4520 cmdline: wmic SHADOWCOPY DELETE /nointeractive MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
  - conhost.exe (PID: 5876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- WMIC.exe (PID: 4800 cmdline: wmic SHADOWCOPY DELETE /nointeractive MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
  - conhost.exe (PID: 4768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- WMIC.exe (PID: 3148 cmdline: wmic SHADOWCOPY DELETE /nointeractive MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
  - conhost.exe (PID: 1756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ab.exe (PID: 1864 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe MD5: 0B486FE0503524CFE4726A4022FA6A68)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\uCLrcwQ_readme_.txt	JoeSecurity_Avaddon	Yara detected Avaddon Ransomware	Joe Security	
C:\Users\Public\Libraries\uCLrcwQ_readme_.txt	JoeSecurity_Avaddon	Yara detected Avaddon Ransomware	Joe Security	
C:\Users\Public\Libraries\uCLrcwQ_readme_.txt	JoeSecurity_Avaddon	Yara detected Avaddon Ransomware	Joe Security	
C:\Users\Public\Libraries\uCLrcwQ_readme_.txt	JoeSecurity_Avaddon	Yara detected Avaddon Ransomware	Joe Security	
C:\Users\Public\Libraries\uCLrcwQ_readme_.txt	JoeSecurity_Avaddon	Yara detected Avaddon Ransomware	Joe Security	
Click to see the 7 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.317257973.00000000043E8000.00000004.00000010.sdmp	JoeSecurity_Avaddon	Yara detected Avaddon Ransomware	Joe Security	
00000000.00000003.316985824.00000000043E8000.00000004.00000010.sdmp	JoeSecurity_Avaddon	Yara detected Avaddon Ransomware	Joe Security	
00000000.00000003.324241984.00000000007E5000.00000004.00000001.sdmp	JoeSecurity_PersistenceViaHiddenTask	Yara detected PersistenceViaHiddenTask	Joe Security	
00000000.00000003.324241984.00000000007E5000.00000004.00000001.sdmp	JoeSecurity_Avaddon	Yara detected Avaddon Ransomware	Joe Security	
00000000.00000003.315481275.00000000007E5000.00000004.00000001.sdmp	JoeSecurity_PersistenceViaHiddenTask	Yara detected PersistenceViaHiddenTask	Joe Security	
Click to see the 18 entries				

Sigma Overview

System Summary:

Sigma detected: Shadow Copies Deletion Using Operating Systems Utilities

Sigma detected: Copying Sensitive Files with Credential Data

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Spreading:

Spreads via windows shares (copies files to share folders)

Copyright Joe Security LLC 2022

Spam, unwanted Advertisements and Ransom Demands:

- Yara detected Avaddon Ransomware
- Found ransom note / readme
- Yara detected RansomwareGeneric
- Modifies existing user documents (likely ransomware behavior)
- Deletes shadow drive data (may be related to ransomware)

System Summary:

Persistence and Installation Behavior:

- Yara detected PersistenceViaHiddenTask
- Creates processes via WMI

Boot Survival:

- Yara detected PersistenceViaHiddenTask

Anti Debugging:

- Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

Lowering of HIPS / PFW / Operating System Security Settings:

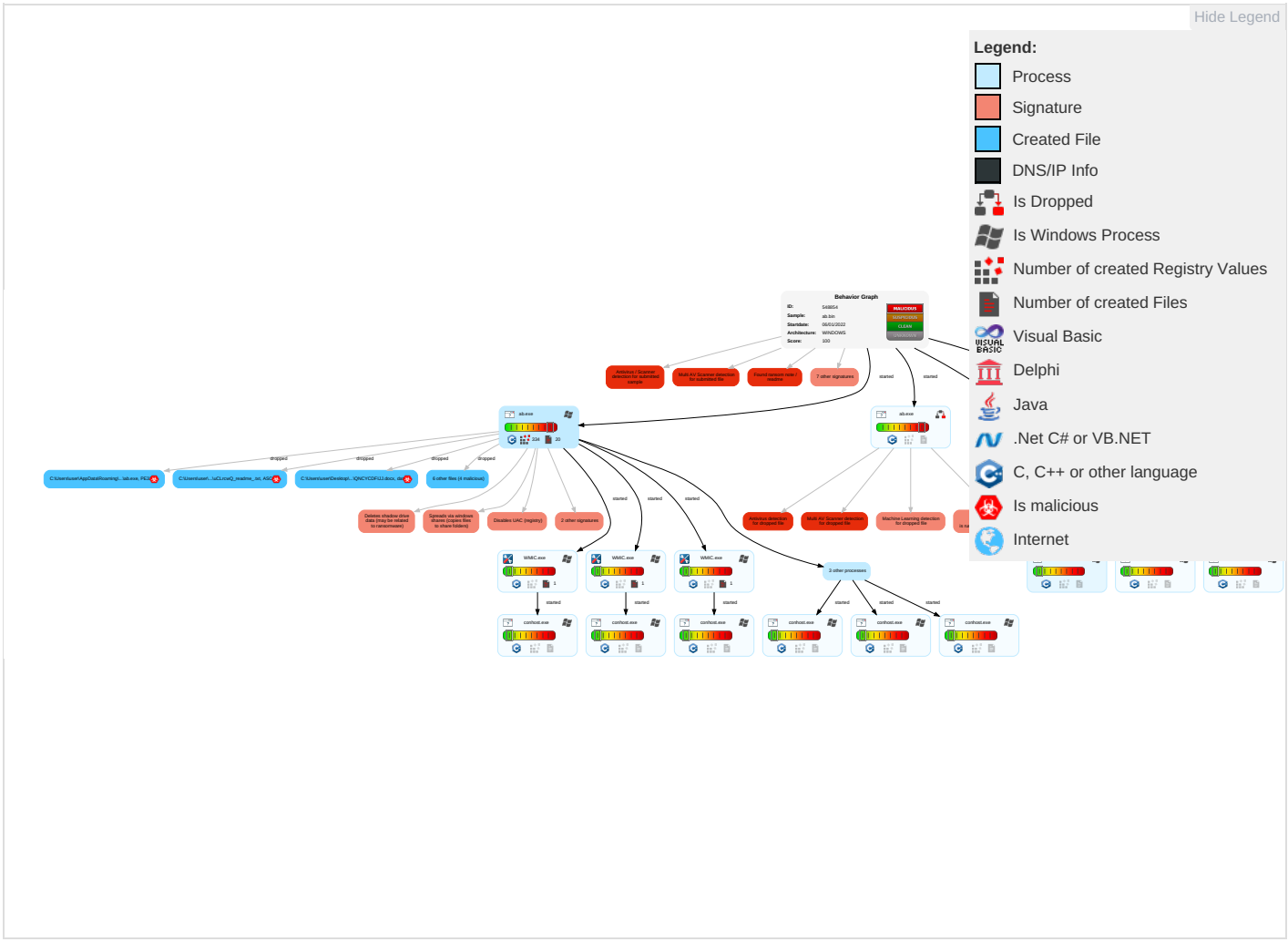
- Disables UAC (registry)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Replication Through Removable Media 1	Windows Management Instrumentation 1 1	Windows Service 1 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	System Time Discovery 2	Taint Shared Content 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Windows Service 1 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 4 1	Replication Through Removable Media 1	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Ex Re Ca
Domain Accounts	Service Execution 1 2	DLL Side-Loading 1	Process Injection 1 1	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Ex Tr Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Access Token Manipulation 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	Sl Sv
Cloud Accounts	Cron	Network Logon Script	DLL Side-Loading 1	Process Injection 1 1	LSA Secrets	Peripheral Device Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 3 7	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do Ins Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rc Ba

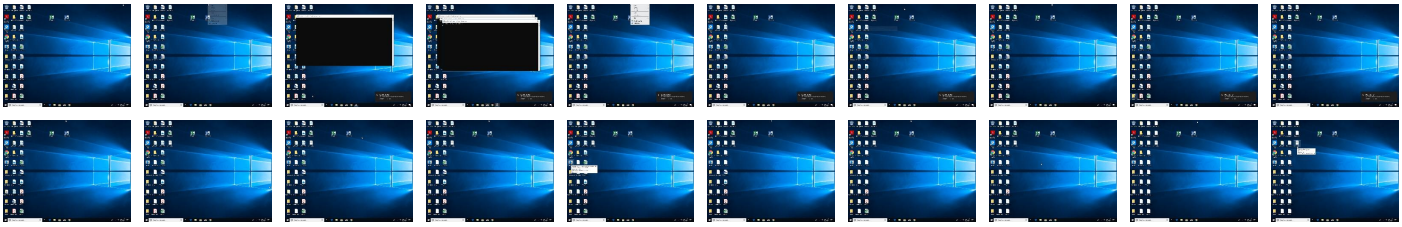
Behavior Graph

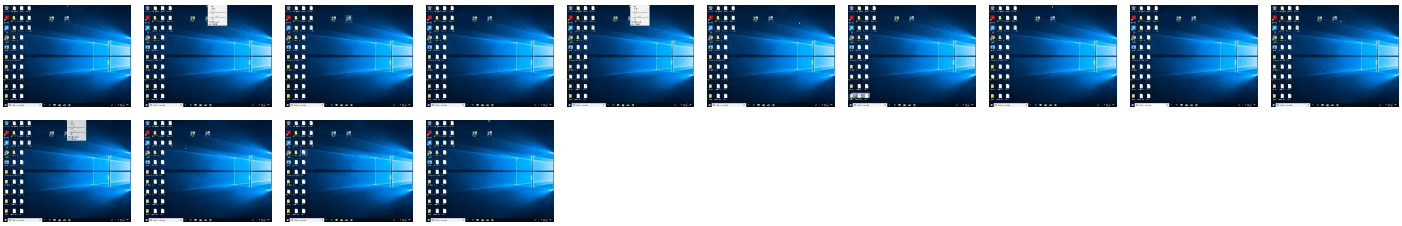


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ab.exe	88%	Virustotal		Browse
ab.exe	66%	Metadefender		Browse
ab.exe	96%	ReversingLabs	Win32.Ransomware.Avaddon	
ab.exe	100%	Avira	HEUR/AGEN.1136765	
ab.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe	100%	Avira	HEUR/AGEN.1136765	
C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe	100%	Joe Sandbox ML		

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe	88%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe	66%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe	96%	ReversingLabs	Win32.Ransomware.Avaddon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
35.0.ab.exe.12f0000.0.unpack	100%	Avira	HEUR/AGEN.1136765		Download File
0.0.ab.exe.10e0000.0.unpack	100%	Avira	HEUR/AGEN.1136765		Download File
2.0.ab.exe.12f0000.0.unpack	100%	Avira	HEUR/AGEN.1136765		Download File
2.2.ab.exe.12f0000.0.unpack	100%	Avira	HEUR/AGEN.1136765		Download File
35.2.ab.exe.12f0000.0.unpack	100%	Avira	HEUR/AGEN.1136765		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.torproject.o	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	548854
Start date:	06.01.2022
Start time:	16:46:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ab.bin (renamed file extension from bin to 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:	45
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

Copyright Joe Security LLC 2022

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.spre.troj.evad.winEXE@27/228@0/0
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 36.1% (good quality ratio 34.5%) • Quality average: 67.8% • Quality standard deviation: 26.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:47:35	Task Scheduler	Run new task: update path: C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe
16:47:36	API Interceptor	6x Sleep call for process: WMIC.exe modified
16:47:46	API Interceptor	1x Sleep call for process: ab.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\$RECYCLE.BIN\S-1-5-21-3853321935-2125563209-4053062332-1002\desktop.ini	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	Windows desktop.ini, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	129
Entropy (8bit):	5.323600488446077
Encrypted:	false
SSDEEP:	3:0NdQDjoqxyRVIQBU+1IVLfAPmBACaWZcy/FbBmedyn:0NwoSyzI2U8MAPVCawbBmeUn
MD5:	A526B9E7C716B3489D8CC062FBCE4005
SHA1:	2DF502A944FF721241BE20A9E449D2ACD07E0312

C:\$RECYCLE.BIN\S-1-5-21-3853321935-2125563209-4053062332-1002\desktop.ini	
SHA-256:	E1B9CE9B57957B1A0607A72A057D6B7A9B34EA60F3F8AA8F38A3AF979BD23066
SHA-512:	D83D4C656C96C3D1809AD06CE78FA09A77781461C99109E4B81D1A186FC533A7E72D65A4CB7EDF689EECCDA8F687A13D3276F1111A1E72F7C3CD92A49BCE0F8
Malicious:	false
Preview:	[.ShellClassInfo]..CLSID={645FF040-5081-101B-9F08-00AA002F954E}..LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-8964..

C:\$RECYCLE.BIN\desktop.ini	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	Windows desktop.ini, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	129
Entropy (8bit):	5.323600488446077
Encrypted:	false
SSDEEP:	3:0NdQDjoqxyRVIQBU+1IVLfAPmBACaWZcy/FbBmedyn:0NwoSyzI2U8MAPVCawbBmeUn
MD5:	A526B9E7C716B3489D8CC062FBCE4005
SHA1:	2DF502A944FF721241BE20A9E449D2ACD07E0312
SHA-256:	E1B9CE9B57957B1A0607A72A057D6B7A9B34EA60F3F8AA8F38A3AF979BD23066
SHA-512:	D83D4C656C96C3D1809AD06CE78FA09A77781461C99109E4B81D1A186FC533A7E72D65A4CB7EDF689EECCDA8F687A13D3276F1111A1E72F7C3CD92A49BCE0F8
Malicious:	false
Preview:	[.ShellClassInfo]..CLSID={645FF040-5081-101B-9F08-00AA002F954E}..LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-8964..

C:\Users\Public\Libraries\RecordedTV.library-ms	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97920677738626
Encrypted:	false
SSDEEP:	192:AmnF2WNC7nuVmW/CKw3GwU+GpV0nD2t6SOtpVD4sNK763dV+P:321W/nwWwU+GpeD20rissGO
MD5:	E22DCB2757FF27EEF3268FB5726335A2
SHA1:	CAC1831D5DDC0D5FCB743AC5570FB501DCB1A49A
SHA-256:	299386AACAF3CDA22C4DF4647593E644DBB668BCC2DA4B4D3B41BB98E43AF428
SHA-512:	1D99E98BF756EF952695C5552ABDB06B74720825DAFF8ECBF0D72311B4303F6E8013C8515BB3EDAB698D0D6271AE2A5D06B6CE0FF0DECC5FD438366B374ECAB8
Malicious:	false
Preview:	.]..f.).....K...u[[G.ZX.!.|K.b.B.B.Pv...#.l..EgK5.....a..I....BN..TP...E]..g.fr...W...._.2#F...I.@.f}qf*..@N....."....&n.p...tb/..y.<.....?O.....o..dh,%...>...$Jy...a.....]--..#&.....W.b....\..a.....@W -K.5,....j.....~.T....<..N..J..~..M...+...GP.'+.L..:3...w.....{.{.I..$d..5..-.-.M)3CD.....e.H...../..<...#._V....Mgn..U..7.u...~...o0.....!<....A#.t~.fJ|.:.5.k...f=..W..t.....*]...S.W.....V.."..M..9.w.....O....6..7p..7.Sj.I^i.{....H...P5...,..&m...H..G;z1i....N..+..b.....u..X.h..fU...@.j.ix..>T.I....G..s....i.....f&yH..5....!.,K/.'%^.|.[.....:E.....E..8.".u.@c.....[.@U.d....hK..@4..(....O..f..@^.S.G..e.]..*F.Y..Qo..W...U.I..C...<76.vzyJ? ..,.I,}....p+j,.....s....V.xn.e../.x...HP.7v...W;.>....n.M.L..G3L."J...N.w.f....a.o.....W..".?.h.Mt.v....l..p..K....1..#.I.....k....r.....W....5...=*63e<.....E.\...^=....y..z.....E45.\T...'.]...W8..m#<..4..,_.I..^*I.S..tn....@F..%!/NT.{..:.../p.-n,.5*.|...W..

C:\Users\Public\Libraries\RecordedTV.library-ms.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97920677738626
Encrypted:	false
SSDEEP:	192:AmnF2WNC7nuVmW/CKw3GwU+GpV0nD2t6SOtpVD4sNK763dV+P:321W/nwWwU+GpeD20rissGO
MD5:	E22DCB2757FF27EEF3268FB5726335A2
SHA1:	CAC1831D5DDC0D5FCB743AC5570FB501DCB1A49A
SHA-256:	299386AACAF3CDA22C4DF4647593E644DBB668BCC2DA4B4D3B41BB98E43AF428
SHA-512:	1D99E98BF756EF952695C5552ABDB06B74720825DAFF8ECBF0D72311B4303F6E8013C8515BB3EDAB698D0D6271AE2A5D06B6CE0FF0DECC5FD438366B374ECAB8
Malicious:	false
Preview:	.]..f.).....K...u[[G.ZX.!.|K.b.B.B.Pv...#.l..EgK5.....a..I....BN..TP...E]..g.fr...W...._.2#F...I.@.f}qf*..@N....."....&n.p...tb/..y.<.....?O.....o..dh,%...>...$Jy...a.....]--..#&.....W.b....\..a.....@W -K.5,....j.....~.T....<..N..J..~..M...+...GP.'+.L..:3...w.....{.{.I..$d..5..-.-.M)3CD.....e.H...../..<...#._V....Mgn..U..7.u...~...o0.....!<....A#.t~.fJ|.:.5.k...f=..W..t.....*]...S.W.....V.."..M..9.w.....O....6..7p..7.Sj.I^i.{....H...P5...,..&m...H..G;z1i....N..+..b.....u..X.h..fU...@.j.ix..>T.I....G..s....i.....f&yH..5....!.,K/.'%^.|.[.....:E.....E..8.".u.@c.....[.@U.d....hK..@4..(....O..f..@^.S.G..e.]..*F.Y..Qo..W...U.I..C...<76.vzyJ? ..,.I,}....p+j,.....s....V.xn.e../.x...HP.7v...W;.>....n.M.L..G3L."J...N.w.f....a.o.....W..".?.h.Mt.v....l..p..K....1..#.I.....k....r.....W....5...=*63e<.....E.\...^=....y..z.....E45.\T...'.]...W8..m#<..4..,_.I..^*I.S..tn....@F..%!/NT.{..:.../p.-n,.5*.|...W..

C:\Users\Public\Libraries\uCLrcwQ_readme_.txt	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators

C:\Users\Public\Libraries\uCLrcwQ_readme_.txt

Category:	modified
Size (bytes):	3777
Entropy (8bit):	5.732654072634773
Encrypted:	false
SSDEEP:	48:L9k0ZzV7L/vNbXGZULVDgUp4qNiiE6bm1c0rfWejhAe/YAliM3PXnLHrYxgkH69J:L95zhLNbXGZUe7Ka6pU6i9fLrvE69USd
MD5:	7C4A65CA4999BD0122440C05C4D40942
SHA1:	8494FA2322AF44C66F598179B42D08105374AD6F
SHA-256:	86DFF7E4B80C8A48CC63CB4A0DFC3B92C64355E9B441B3D3C05EE319A25FBFF0
SHA-512:	A61FA1744DB62E97A448ADF564A162D61CD10DE6BC03734369BDA58D32AAB67B81F18667B5E5842DF57672E009385AE03ED5868354732F61CDD0B3B27C60696
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: C:\Users\Public\Libraries\uCLrcwQ_readme_.txt, Author: Joe Security
Preview:	-------=== Your network has been infected! ===-------.........****************** DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED **** *************.........All your documents, photos, databases and other important files have been encrypted and have the extension: .bCcBDeabea......You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!......The only way to restore your files is to buy our special software. Only we can give you this software and only we can restore your files!......We have also downloaded a lot of private data from your network....If you do not contact as in a 3 days we will post information about your breach on our public news website (avaddongun7rngel.onion) and after 7 days the whole downloaded info.......You can get more information on our page, which is located in a Tor hidden network.........How to get to our page...---

C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe

Process:	C:\Users\user\Desktop\ab.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	794112
Entropy (8bit):	6.16411908069709
Encrypted:	false
SSDEEP:	24576:TCs99+OXLpMePfI8TgmBTCDqEbOpPtpFhyxfq:5GOXLpMePfzVTCD7gPtLhSfq
MD5:	0B486FE0503524CFE4726A4022FA6A68
SHA1:	297DEA71D489768CE45D23B0F8A45424B469AB00
SHA-256:	1228D0F04F0BA82569FC1C0609F9FD6C377A91B9EA44C1E7F9F84B2B90552DA2
SHA-512:	F4273CA5CC3A9360AF67F4B4EE0BF067CF218C5DC8CAEAFBFA1B809715EFFE742F2E1F54E4FE9EC8D4B8E3AE697D57F91C2B49BDF203648508D75D4A76F536 19
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 88%, Browse • Antivirus: Metadefender, Detection: 66%, Browse • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......9.I.}.'}}.'}i.$|I.'}i."|.'}i.#|j.'}i.!|..'}..#|I.'}..$|k.'}.."|.'}i.&|j.'}}.&}..'}...|I.'}...}|.'}}..}|.'}..%||.'}Rich}.'}................PE..L...G.h`.................*..................@....@..........................`...........@................................. ....D...,n..8.................hn..@............@..X............................text...L(.......*................. ..`.rdata.......@......................@..@.data....x...@...h...".............@....rsrc...............................@..@.r eloc..D..........................@..B... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\ab.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Copyright Joe Security LLC 2022

C:\Users\user\Desktop\BNAGMGSPLO.jpg	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978845042070389
Encrypted:	false
SSDEEP:	192:Cw8bRbuj/mAcfzOaMdsonbziYvSHsj/4a57yV+n:CZlVAcfzOxNnbT6etr
MD5:	C1DD5D9DDD42B96F8CB33309E8E5E313
SHA1:	DA232AE8830066BFE4689BFC22641E5E966DCA38
SHA-256:	35E5F4EE17A317C29EA205854051061007F8CB7B1C1480F8F45F11AA8FB3CC4D
SHA-512:	61DD30A3F328A8D8DFFCF0908F9E91AF224CD1FD485C69D5809EFD4D00DDCEC2933B32C4FEB946BDFE5E0F0CD82A7FBA9E6DBFEDEFA9C0B1D43C2734211879B
Malicious:	**true**
Preview:	6.u...tXP+(.\..;@8.q`.c....OE...A.....}.C.'PQ..`VX./.fdSO.a.b.b!..4..By...../..]kX..;.....o....^..6..[.9. d.....~.l.I..w$T.....1.....$$....A.u.D..O.^b.vi...a.;Lp:..PV2.....V...`...#WC.....s.k..?...~....n.....'.P`."..o..r....S..K.....Y..k32".rH...2G.w...:$...l%-.$F..t.fEy.....j.a.....)uR.....HRAn.....z.@..i....i.....g8@.....} ...+p..(.....!\..[.{#<nuP.y.....,.d..l6d../l%8...X.h.....f(I<.@.ca...+.6../."`....4-y.n.`..PY`..+o:yZA0{..L.`.n.pS..g.!#h1.pP.X..i.i.....%...6h.P:.88.AHrJ~...x.E..kp=B.....}..{.m.W.....9P~....P..o..h..#.....x.1.8....4.V#^..0....}.s..;...i...d...%..SWy.Vc.\....3...B.V.K....J.....{1Q...G6$..^.~iOh...5:...@.)..N.eN.:e.k.A..8O.....G..a....=...A...bC.e...gq\...9.ok(..v.().>.^A....yn.n..q..y....~..m.....25ZKX./X\P.!.B8.....0j.;..FY.]L.k.xt.?.arI.r...m=....|Ly.n.~&....tt..8.:V.5".....y.>.....QKd...x..k..k...s.<.}x..d....}F..%.m.....v...Z.._.....8..}A.e..%./...L.n...}....9.

C:\Users\user\Desktop\BNAGMGSPLO.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978845042070389
Encrypted:	false
SSDEEP:	192:Cw8bRbuj/mAcfzOaMdsonbziYvSHsj/4a57yV+n:CZlVAcfzOxNnbT6etr
MD5:	C1DD5D9DDD42B96F8CB33309E8E5E313
SHA1:	DA232AE8830066BFE4689BFC22641E5E966DCA38
SHA-256:	35E5F4EE17A317C29EA205854051061007F8CB7B1C1480F8F45F11AA8FB3CC4D
SHA-512:	61DD30A3F328A8D8DFFCF0908F9E91AF224CD1FD485C69D5809EFD4D00DDCEC2933B32C4FEB946BDFE5E0F0CD82A7FBA9E6DBFEDEFA9C0B1D43C2734211879B
Malicious:	false
Preview:	6.u...tXP+(.\..;@8.q`.c....OE...A.....}.C.'PQ..`VX./.fdSO.a.b.b!..4..By...../..]kX..;.....o....^..6..[.9. d.....~.l.I..w$T.....1.....$$....A.u.D..O.^b.vi...a.;Lp:..PV2.....V...`...#WC.....s.k..?...~....n.....'.P`."..o..r....S..K.....Y..k32".rH...2G.w...:$...l%-.$F..t.fEy.....j.a.....)uR.....HRAn.....z.@..i....i.....g8@.....} ...+p..(.....!\..[.{#<nuP.y.....,.d..l6d../l%8...X.h.....f(I<.@.ca...+.6../."`....4-y.n.`..PY`..+o:yZA0{..L.`.n.pS..g.!#h1.pP.X..i.i.....%...6h.P:.88.AHrJ~...x.E..kp=B.....}..{.m.W.....9P~....P..o..h..#.....x.1.8....4.V#^..0....}.s..;...i...d...%..SWy.Vc.\....3...B.V.K....J.....{1Q...G6$..^.~iOh...5:...@.)..N.eN.:e.k.A..8O.....G..a....=...A...bC.e...gq\...9.ok(..v.().>.^A....yn.n..q..y....~..m.....25ZKX./X\P.!.B8.....0j.;..FY.]L.k.xt.?.arI.r...m=....|Ly.n.~&....tt..8.:V.5".....y.>.....QKd...x..k..k...s.<.}x..d....}F..%.m.....v...Z.._.....8..}A.e..%./...L.n...}....9.

C:\Users\user\Desktop\EEGWXUHVUG.png	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978111793832275
Encrypted:	false
SSDEEP:	192:OkGcTe/5yk671S6mqkBeSv4SXq407EzQyXvkwrGV+n:51Bk6RS6nQXxHEEz5
MD5:	E4C6DDAC88526D3CC6861A9E4279477B
SHA1:	4C9F8F0987306CB664E26B9FAACDA969451C0CFE
SHA-256:	B572F5CDFCFC14CDFCD5938B1E63E599CC0C7C2DAAF22A48AC7BA03969802B2C
SHA-512:	EC68AB52A5A3BB66CB59895ACFD7ACB2B8B084F4C410DD4D48E9306F6162CADA7F8857F1567FC84AB899ECA10F2F4B9C1D1651DA3B3F6ABE09BFD67C3D8EACFA
Malicious:	false
Preview:	F...6.4.ka{.T.Mx].....%.34...'+*.f.....L.D.D.#.V.q..%.....f.|rF.p....4O.../...:..P2.0.@{Y.....p.n..2..>.G..L$.....w.)g.'..6V.}1A<..Q.....}..~@.....j.].....)...d.e.....D.._+..K.$...qS..<]d.:.....E.y.D.....s.....".....;}..]}D.p@..$..jl.N.;.D\`....)7....j...Nr...{...M...W...3.....l[z....NU.p..y.P..U.?VQ.....k+...T...z.n....g..m)...K>)..h.&*4..<j.$1~.U.....8f.R....Zg..S...S.Le..{..85.....n@.7..mrh&.G.....m .}.x.....R.-..y.Eh/.....w...3.....f.....n..M.!.....v...c.2..Q.Fp.....8..1....V.m.....].+7..X.c..B.....!P....j...I..wu'.R.:.....Z.6c.#^IS...../..P.2#...d..^H.U.WJ"..o.,.<..?...fn"$C.]..kC.b.d.r.fp../..L....v&,;h...Z..h%...2.....s....].T.-.'...(#+4L.s..2....e$.....y.B.i.L._j&...b...._....c.h{.....p....7.C....,tW ....Q.R....>W....ss..]w..:,.G.....~z.\.Z..DswP.....'[&.uF2%2u..x.*!.%....MXY.dS.K...s.....)L~...._.....b..U1a.P..g7.H\".Am6....._^....dB..'....].Z.R6=..v{....I..q.?..?...ywX.B>8...g....n;.....%Y.

C:\Users\user\Desktop\EEGWXUHVUG.png.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978111793832275
Encrypted:	false

C:\Users\user\Desktop\EEGWXUHVUG.png.bCcBDeabea (copy)	
SSDEEP:	192:OkGcTe/5yk671S6mqkBeSv4SXq407EzQyXvkwrGV+n:51Bk6RS6nQXxHEEz5
MD5:	E4C6DDAC88526D3CC6861A9E4279477B
SHA1:	4C9F8F0987306CB664E26B9FAACDA969451C0CFE
SHA-256:	B572F5CDFCFC14CDFCD5938B1E63E599CC0C7C2DAAF22A48AC7BA03969802B2C
SHA-512:	EC68AB52A5A3BB66CB59895ACFD7ACB2B8B084F4C410DD4D48E9306F6162CADA7F8857F1567FC84AB899ECA10F2F4B9C1D1651DA3B3F6ABE09BFD67C3D8EA CFA
Malicious:	false
Preview:	F...6.4.ka{.T.Mx].....%.34...'+*..f.....L.D.D.#.V.q..%.....f.|rF.p....4O.../..:..P2.0.@{Y.....p.n..2..>.G..L$.....w.)g.'..6V.}1A<..Q.....}..~@.....j.].....)...d.e.....D.._+..K.$...qS..<]d.:. ...E.y.D.....s.....".....;}..]}D.p@..$..jl.N.;.D\`....)7.....j...Nr...{...M...W...3.....l[z....NU.p..y.P..U.?VQ.....k+...T...z.n....g..m)...K>)..h.&*4..<j.$1~.U.....8f.R....Zg..S...S.Le..{..85. ....n@.7..mrh&.G.....m .}.x.....R.-..y.Eh/.....w...3.....f.....n..M.!.....v...c.2..Q.Fp.....8..1....V.m.....].+7..X.c..B.....!P....j...I..wu'.R.:.....Z.6c.#^IS...../..P.2#...d..^H.U.WJ"..o.,. <..?...fn"$C.]..kC.b.d.r.fp../..L....v&,;h...Z..h%...2.....s....].T.-.'...(#+4L.s..2....e$.....y.B.i.L._j&...b...._....c.h{.....p....7.C....,tW ....Q.R....>W....ss..]w..:,.G.....~z.\.Z..DswP. ...'[&.uF2%2u..x.*!.%....MXY.dS.K...s.....)L~...._.....b..U1a.P..g7.H\".Am6....._.^....dB..'....].Z.R6=..v{....I..q.?..?...ywX.B>8...g....n;.....%Y.

C:\Users\user\Desktop\EFOYFBOLXA.jpg	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9783433145335865
Encrypted:	false
SSDEEP:	192:jCtyPOg9Ta7xm/sJ1duqSNYHTF1DCn03s3nc6JV+n:Ot+qxm/q1dO+zqn8Oc6W
MD5:	264BDCF39559FE6FDB92CFF7582810F1
SHA1:	E21157DCF3F6233446D5A7AC465C52B64704DAB0
SHA-256:	7A6F1A1E0FA03F69A2CA49411ABFFD270C1EED058355F08F1A0AF3B09313C275
SHA-512:	A87784AF608B94445AB2C7D1B4EED2E16F9AF25FAEE50561A3A2A4F059565CFE0FD79538C590CD67212874055458E2DA9858BA8C1D5A5430A82C264ACEC596E
Malicious:	false
Preview:	t.c{Yw..+.JN...5[.i9..b..".[D..7...S.....tl'.$..M..R.7...i.."~...@.n...m..A ?\|....E]...*J..ahb8B....m.u.....xQ.l.).a@.....v..rR.M0.....%..>..pKI._.-.c..%.2.[z?Z~.J.T.X.....\|E .@...N ..ckIb\..{..c..b.u".....l.....{.....E;.MD.....+{.....E!k..D.B4.}".}.....+m.;.Q7....]%.Q...Z3...\|..../.....F..l...M.....e.....2.>Kc.$:u.R..;+.....pNT...W.H#.Zk.SX.CF.~...t.P.l.n|...../... {.Yco.`y$6.GsSv{7y..y.@...yd...(._N...m0!.Y.....)....._...XWD....9..s...;.....f.yr.h.4.c!S@..'....z...<.T'.....3....{.U..pTX.s.%.^.\M.m..S)Y.-..V.HW?.....P.q....v.~....190..V.}..k.sW7 .7..M.?.b.H.N.1-l.....M..6...m._.Z..H..H.Y..j..\.....7.....t.#..=...<.'q...\iv..V'\|.81.K.).6.....f.,.....`NRIx4y4{.s... I..V..G.r..Ql.#B.....3...W`.(..f.....2.kM.....E8^..j..o....d.H,....E....Z ..4$.}_-?....VZ.....UA.S.x....[.....{7%....}..>..2O`fs..7...+.9.9.E6..%.].o...{.....L..`@f.....G>.;.d....%...l..c..7..P....r..T.`.....]....R.F.:.n?_D.l.V. .n.+O

C:\Users\user\Desktop\EFOYFBOLXA.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9783433145335865
Encrypted:	false
SSDEEP:	192:jCtyPOg9Ta7xm/sJ1duqSNYHTF1DCn03s3nc6JV+n:Ot+qxm/q1dO+zqn8Oc6W
MD5:	264BDCF39559FE6FDB92CFF7582810F1
SHA1:	E21157DCF3F6233446D5A7AC465C52B64704DAB0
SHA-256:	7A6F1A1E0FA03F69A2CA49411ABFFD270C1EED058355F08F1A0AF3B09313C275
SHA-512:	A87784AF608B94445AB2C7D1B4EED2E16F9AF25FAEE50561A3A2A4F059565CFE0FD79538C590CD67212874055458E2DA9858BA8C1D5A5430A82C264ACEC596E
Malicious:	false
Preview:	t.c{Yw..+.JN...5[.i9..b..".[D..7...S.....tl'.$..M..R.7...i.."~...@.n...m..A ?\|....E]...*J..ahb8B....m.u.....xQ.l.).a@.....v..rR.M0.....%..>..pKI._.-.c..%.2.[z?Z~.J.T.X.....\|E .@...N ..ckIb\..{..c..b.u".....l.....{.....E;.MD.....+{.....E!k..D.B4.}".}.....+m.;.Q7....]%.Q...Z3...\|..../.....F..l...M.....e.....2.>Kc.$:u.R..;+.....pNT...W.H#.Zk.SX.CF.~...t.P.l.n|...../... {.Yco.`y$6.GsSv{7y..y.@...yd...(._N...m0!.Y.....)....._...XWD....9..s...;.....f.yr.h.4.c!S@..'....z...<.T'.....3....{.U..pTX.s.%.^.\M.m..S)Y.-..V.HW?.....P.q....v.~....190..V.}..k.sW7 .7..M.?.b.H.N.1-l.....M..6...m._.Z..H..H.Y..j..\.....7.....t.#..=...<.'q...\iv..V'\|.81.K.).6.....f.,.....`NRIx4y4{.s... I..V..G.r..Ql.#B.....3...W`.(..f.....2.kM.....E8^..j..o....d.H,....E....Z ..4$.}_-?....VZ.....UA.S.x....[.....{7%....}..>..2O`fs..7...+.9.9.E6..%.].o...{.....L..`@f.....G>.;.d....%...l..c..7..P....r..T.`.....]....R.F.:.n?_D.l.V. .n.+O

C:\Users\user\Desktop\EFOYFBOLXA.mp3	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9745453799453605
Encrypted:	false
SSDEEP:	192:rAbd0iWYRBCS4u2uVMMLx9PBUaLx64Cqv3Chz/kYVV+n:wdfHf94upqMl9PBUQxh3v3uz/a
MD5:	EC542B434FA48D85DC67F32EB751A4E3
SHA1:	B2620AB705E48FE29352AD8EDE11933C7F9D6B5F
SHA-256:	C3D00E5448E4C971F8CA65F0514C3A579E32D9AB51CBC00217540B6F6BBC6A96
SHA-512:	13D585F8E8C3BFB3780A4127E94C61E1530E357A97111CFE237DC6057A485CCADB46378275F437D60A2F6655B5A1E8C3B4F2C9FFE027B859D0C2CDB0877F2A7
Malicious:	false

C:\Users\user\Desktop\EFOYFBOLXA.mp3	
Preview:	.....+=52_....>W.H..z.:.l.;.`.....^.....lU.].....HA.....4.v...|.]..:.;.J..h.....#b....;./R.r.s..f//f}.......q....&4...@..&x..x{..1....:[]u;.{.........(a.KJ.K/.w.%.k..1]6p.w&..^O.g.).1G...I...3|>oY... ..T...m..$..."4.6t...4..T.L...W.C.8H..`.kI.o.........Bu.+...D.Rz.....!S..#.x..*._.[.R.)i.mO.L`}.pk*..1..).....,by...B..:.. 0g.....W.... .(..Y...."..L...9<.*.....;;..m.q:..S....o.0.t.LOT..X".#K.....{ ...p.5..V..$a.&...[^O].r.'VE1*<UD..#`.d.e..U0.6.....n...S....%`.....vY"..7.[....|.m.....n.=okp?..:.....>r..qU~<.H.....8.W..m.....,_....Ai..q.}..P..5..#.C...y?.-.c.....O.(}c.^\.F...Z..... M.O=p...2.k.hUK...9.N`.Q.Q.(..m.....T.c9.|..%w.+u`4g<..N..._...}k.C....U.....Ah I.....-BM..f..kI.>...%.?!.p.q....*P...[.a5e....-.!g.Hh..l...D....r..Q...?o..Z.e..&=..R.Jd.nj.W..E.f...A.....q ._vB........~.....$# ...2j. .5.{BQ...+..3l....6..;.}...5.._...H...s..eS....(._.X....'j.{.Lj.@.96k..l..G(P.1+..ww|6.....O%........FU.e..x.`r.....L.S.7.q.....Lk.N....2lkE.....Q.g#.w.

C:\Users\user\Desktop\EFOYFBOLXA.mp3.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9745453799453605
Encrypted:	false
SSDEEP:	192:rAbd0iWYRBCS4u2uVMMLx9PBUaLx64Cqv3Chz/kYVV+n:wdfHf94upqMl9PBUQxh3v3uz/a
MD5:	EC542B434FA48D85DC67F32EB751A4E3
SHA1:	B2620AB705E48FE29352AD8EDE11933C7F9D6B5F
SHA-256:	C3D00E5448E4C971F8CA65F0514C3A579E32D9AB51CBC00217540B6F6BBC6A96
SHA-512:	13D585F8E8C3BFB3780A4127E94C61E1530E357A97111CFE237DC6057A485CCADB46378275F437D60A2F6655B5A1E8C3B4F2C9FFE027B859D0C2CDB0877F2A7
Malicious:	false
Preview:	.....+=52_....>W.H..z.:.l.;.`.....^.....lU.].....HA.....4.v...|.]..:.;.J..h.....#b....;./R.r.s..f//f}.......q....&4...@..&x..x{..1....:[]u;.{.........(a.KJ.K/.w.%.k..1]6p.w&..^O.g.).1G...I...3|>oY... ..T...m..$..."4.6t...4..T.L...W.C.8H..`.kI.o.........Bu.+...D.Rz.....!S..#.x..*._.[.R.)i.mO.L`}.pk*..1..).....,by...B..:.. 0g.....W.... .(..Y...."..L...9<.*.....;;..m.q:..S....o.0.t.LOT..X".#K.....{ ...p.5..V..$a.&...[^O].r.'VE1*<UD..#`.d.e..U0.6.....n...S....%`.....vY"..7.[....|.m.....n.=okp?..:.....>r..qU~<.H.....8.W..m.....,_....Ai..q.}..P..5..#.C...y?.-.c.....O.(}c.^\.F...Z..... M.O=p...2.k.hUK...9.N`.Q.Q.(..m.....T.c9.|..%w.+u`4g<..N..._...}k.C....U.....Ah I.....-BM..f..kI.>...%.?!.p.q....*P...[.a5e....-.!g.Hh..l...D....r..Q...?o..Z.e..&=..R.Jd.nj.W..E.f...A.....q ._vB........~.....$# ...2j. .5.{BQ...+..3l....6..;.}...5.._...H...s..eS....(._.X....'j.{.Lj.@.96k..l..G(P.1+..ww|6.....O%........FU.e..x.`r.....L.S.7.q.....Lk.N....2lkE.....Q.g#.w.

C:\Users\user\Desktop\GAOBCVIQIJ.docx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.981497081320176
Encrypted:	false
SSDEEP:	192:qzGrGSjQTt3CLCPLXJQpLOW/uUjQr6Ku3q2KUaf++X7bIIcV+n:qPpT9E45uLf/K2KeeUKfX786
MD5:	3396CC70C716549D807D7369852BCF3F
SHA1:	31D6C6115E391A1874829A2BC8845BB82B129853
SHA-256:	C38479E47FB444B527F74246ECC70EEA27E82F27D5916296115A49706856BD31
SHA-512:	F687B53F93B7105A1472A8CDE059BDA8EF1DE91B0C8DE83095BE834A1597BF404C27D9606CC99705AFA7F3746C533C7F5536808275838FDB8CC6A91566A277C
Malicious:	false
Preview:	.....G..(...~.M...}.@];..c..k.B.....'.F.....W..{.f+.#.Nc..,.$.!...._.%0z.>.k.QX.@f.Z.mS..\.....!...RA...-...\|,\..P.l."...........0..-[]Ff.g.o...3..ks...=X.S...b...{.2'...S5)Kv...T.m.)q..b...I .....k.....S..S.....G.L|..j.i.O..Vy.o....c..)..c.6.]I..4kL.fP..M.9.4.Xe.e&p.....*v...Gq....JxY..Am...H....<^..N....>.....B'Bn...k..bG.$.2.....3.....=.t.T..B.f..[G...BfV3.#:...../..A..~.80 ..l..._...,.a.....[...d...'.....7.....i...<._...SO...{&.{0..&.....i..\A.[.#h".b..|....J.N....X....._.:=e!.k.n...;.Q...M.8,.7.o..-N.}{m_.9.o.....8.K..v.....x.....G.5.....Z.....1J.$l..*4..0E...t..c0Y.?.+..W (.R$.xD.R..C.s.Yd..".....R..0%...ZN.?X..S.~.z....+,.4O..3H.....w..?....f|.$.;.0....o4i...b..../..fD1.u...<..*T'S.~^..1{...KQ...D>.&.^..3...3.~.....:].f..To.....}:..:..#.N..y...h..%.3d. ...f]`}..D....k/.Q.....;\So.8b.....+zR..T.u....&...&.Kj..D...N`.....z4..O...7G.,.MB..%..l.Y.6.....8.....Q.9&i.....fB.W...r|x@4kD3."}..Y^.

C:\Users\user\Desktop\GAOBCVIQIJ.docx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.981497081320176
Encrypted:	false
SSDEEP:	192:qzGrGSjQTt3CLCPLXJQpLOW/uUjQr6Ku3q2KUaf++X7bIIcV+n:qPpT9E45uLf/K2KeeUKfX786
MD5:	3396CC70C716549D807D7369852BCF3F
SHA1:	31D6C6115E391A1874829A2BC8845BB82B129853
SHA-256:	C38479E47FB444B527F74246ECC70EEA27E82F27D5916296115A49706856BD31
SHA-512:	F687B53F93B7105A1472A8CDE059BDA8EF1DE91B0C8DE83095BE834A1597BF404C27D9606CC99705AFA7F3746C533C7F5536808275838FDB8CC6A91566A277C
Malicious:	false
Preview:	.....G..(...~.M...}.@];..c..k.B.....'.F.....W..{.f+.#.Nc..,.$.!...._.%0z.>.k.QX.@f.Z.mS..\.....!...RA...-...\|,\..P.l."...........0..-[]Ff.g.o...3..ks...=X.S...b...{.2'...S5)Kv...T.m.)q..b...I .....k.....S..S.....G.L|..j.i.O..Vy.o....c..)..c.6.]I..4kL.fP..M.9.4.Xe.e&p.....*v...Gq....JxY..Am...H....<^..N....>.....B'Bn...k..bG.$.2.....3.....=.t.T..B.f..[G...BfV3.#:...../..A..~.80 ..l..._...,.a.....[...d...'.....7.....i...<._...SO...{&.{0..&.....i..\A.[.#h".b..|....J.N....X....._.:=e!.k.n...;.Q...M.8,.7.o..-N.}{m_.9.o.....8.K..v.....x.....G.5.....Z.....1J.$l..*4..0E...t..c0Y.?.+..W (.R$.xD.R..C.s.Yd..".....R..0%...ZN.?X..S.~.z....+,.4O..3H.....w..?....f|.$.;.0....o4i...b..../..fD1.u...<..*T'S.~^..1{...KQ...D>.&.^..3...3.~.....:].f..To.....}:..:..#.N..y...h..%.3d. ...f]`}..D....k/.Q.....;\So.8b.....+zR..T.u....&...&.Kj..D...N`.....z4..O...7G.,.MB..%..l.Y.6.....8.....Q.9&i.....fB.W...r|x@4kD3."}..Y^.

C:\Users\user\Desktop\GAOBCVIQIJ.pdf	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data

C:\Users\user\Desktop\GAOBCVIQIJ.pdf	
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978097642317819
Encrypted:	false
SSDEEP:	192:4nSV5PDnJomSb4dP/MZJhVZjMukI18+gyPNPzF8cvZ/ifAoFmV+n:4SVFnJJSUsVZJV1zPRzF5gYGD
MD5:	34225C254118F5947327C09C4B3233EC
SHA1:	BEA8D5DF41168A656ABCF9C573818F275AF0E2B8
SHA-256:	9C6846896C72C0826339AE7D84945D058B5EB1C905BE17DB9DCDD4148B36DCA9
SHA-512:	1C8C97D70A10B3101D5681F1775A5A77BF38E0B4E98B93EEA0FD88ED8E476FD97B7F0CC07E133D8ECC89C0735864FF0955ADE98F354D4C5EA042FFE87222A82 8
Malicious:	false
Preview:	. *4.....B(.B...]..{..&g....~..F....K...../....F?#V..26Q..c.e.|.x.y2.3....yB.....8.m..%8.<c..v..._T..H<...-.E.SU.<...I.Yt..Z.IkW.M.+..._..`..c.....PP..!....8..S<(&o.c..oC. .KhWW.^.?3I$....*. ..h.t.-....mI.........=....a.Jr...}`85Z.\..>.m;i.3}W.....-..q..x7.".@.t.i...p7..HWoO..A.^6.N..<'I.U..-.T.,.U.0..kH{..?.....0k.,^.&t.A..fcL.....E.5...9u.`2..@[6P...B+..'..r....RB.tmP..2.). ..U....'%.w.....(.6.....n.oO\|.I...L.....:.!,..s..T(X.....-&.E..u&DUBX.&uiK....8PZ>F.V+.....T...z.'.....MV..._$.B.....h..... ...9..EQ.I.....P..a:.O../._d....U.i. Kk..:(3FF.x.4.Vs.L._3. c..i=<...$..~{WHO.[f.xv.C..Y .yW7{ |~.R.....U}.....`.....).0.#..'..T[.oh.....qVT.U.5.x.9..D...z2fhv.g~.p.V...Ak.7.....Ga.zP.....C.:....[L.....qVI'o=Ec.}./..>.-...d..U..E..`~....fC.. W.b..".wb.{?:L)...aGy.....|.LE.iJbm|.i7H."]..z.L.H.2....Clj}..[.}..3Fa.....P2....{.....V...Aq.h.i2A..GUy.I..W+.f.G..B..(...]..t....i.3.....P.....x.14..<.n.9.#>L.:..5.....1.c

C:\Users\user\Desktop\GAOBCVIQIJ.pdf.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978097642317819
Encrypted:	false
SSDEEP:	192:4nSV5PDnJomSb4dP/MZJhVZjMukI18+gyPNPzF8cvZ/ifAoFmV+n:4SVFnJJSUsVZJV1zPRzF5gYGD
MD5:	34225C254118F5947327C09C4B3233EC
SHA1:	BEA8D5DF41168A656ABCF9C573818F275AF0E2B8
SHA-256:	9C6846896C72C0826339AE7D84945D058B5EB1C905BE17DB9DCDD4148B36DCA9
SHA-512:	1C8C97D70A10B3101D5681F1775A5A77BF38E0B4E98B93EEA0FD88ED8E476FD97B7F0CC07E133D8ECC89C0735864FF0955ADE98F354D4C5EA042FFE87222A82 8
Malicious:	false
Preview:	. *4.....B(.B...]..{..&g....~..F....K...../....F?#V..26Q..c.e.|.x.y2.3....yB.....8.m..%8.<c..v..._T..H<...-.E.SU.<...I.Yt..Z.IkW.M.+..._..`..c.....PP..!....8..S<(&o.c..oC. .KhWW.^.?3I$....*. ..h.t.-....mI.........=....a.Jr...}`85Z.\..>.m;i.3}W.....-..q..x7.".@.t.i...p7..HWoO..A.^6.N..<'I.U..-.T.,.U.0..kH{..?.....0k.,^.&t.A..fcL.....E.5...9u.`2..@[6P...B+..'..r....RB.tmP..2.). ..U....'%.w.....(.6.....n.oO\|.I...L.....:.!,..s..T(X.....-&.E..u&DUBX.&uiK....8PZ>F.V+.....T...z.'.....MV..._$.B.....h..... ...9..EQ.I.....P..a:.O../._d....U.i. Kk..:(3FF.x.4.Vs.L._3. c..i=<...$..~{WHO.[f.xv.C..Y .yW7{ |~.R.....U}.....`.....).0.#..'..T[.oh.....qVT.U.5.x.9..D...z2fhv.g~.p.V...Ak.7.....Ga.zP.....C.:....[L.....qVI'o=Ec.}./..>.-...d..U..E..`~....fC.. W.b..".wb.{?:L)...aGy.....|.LE.iJbm|.i7H."]..z.L.H.2....Clj}..[.}..3Fa.....P2....{.....V...Aq.h.i2A..GUy.I..W+.f.G..B..(...]..t....i.3.....P.....x.14..<.n.9.#>L.:..5.....1.c

C:\Users\user\Desktop\GAOBCVIQIJ\BNAGMGSPLO.jpg	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97864135938087
Encrypted:	false
SSDEEP:	192:20TaDQLe6Qt5HDpL4xa6UBGXqM3w9Rza1MvChxIDyV+n:202DAeltHLBusG7+H
MD5:	6C40E0A15375AE854B6CCA84EA7916D2
SHA1:	D35BE7C8D002D4606E43EDA9949CB96A1E117C30
SHA-256:	143634615334FA1F670AA65AE0C494668FC5DFD52A36A46EFFB2D7EDAA187107
SHA-512:	E9BC02BC6C0FB766F514B26EADEF41045A9436214CA852F6207AD8633FB52B86DB19E8EC25A920940B996AEA774F47A3A9FD5E80201C35671B6D16A5CBEE7B9 F
Malicious:	false
Preview:	...|B.~"QK%V..0...E*vnu..u.]<...`?)....#.G.....v.....{+.....s`..J.k...#...O..B.....\....<..8f.a.<^o.9Zch."...j.XoeC..h.!..H..|.....k..l..n..0'.....^o..._...^.;.~....+....;.U...&T~:...`..H.Q..CT.. +.Q4F.....L.. .%...._.A.y.....X"...P{.uM...c..k....p.. ..xV.&b2A>f....n._..n.h/#..6....a.H6...p..n.e.fU.P,O...N.....+'G....g.Uu....D...*z.^..A.P..].F.E~.o....}..G..7L..S....s.r....4_D.. .....ibk..1&..F.W...X.....m3GEJ.Gzc..;..J"...[.....o.9..k.2!x.'S..}./=i..u.\X.I.....b(R/Y.a?...,.4_...^..-..FZ..7d.B.=.HY.....x....f(Sax....l..e..CR..f...LvL.3.:.x.v..._'..11.$mq...$. s,p=89..`.... ...L...'..i.....Z.O...f<..;qjM}.p(&...v^.....Ub.a5A..B.....$.....W`/2....p....Je.-...PF.-J.k:.0u.Kx~S'.>.....~. Z.q./.....I.]..~9&..j,..S."..Y....aiY.6Or1.v..dV~.".. y..6!:<.G.....z.^..S.@.Z.pE.s#.+E.I..i.j..p..C..x.C...\.I.z.3".R..G`+...a.h....D!.4e....n....}.....z....0.}dV..<.`.....QMf5.O...J.%f.'Q... .$.Wj.Es..FLE...:..>.....*..].(

C:\Users\user\Desktop\GAOBCVIQIJ\BNAGMGSPLO.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97864135938087
Encrypted:	false
SSDEEP:	192:20TaDQLe6Qt5HDpL4xa6UBGXqM3w9Rza1MvChxIDyV+n:202DAeltHLBusG7+H
MD5:	6C40E0A15375AE854B6CCA84EA7916D2

C:\Users\user\Desktop\GAOBCVIQIJ\BNAGMGSPLO.jpg.bCcBDeabea (copy)	
SHA1:	D35BE7C8D002D4606E43EDA9949CB96A1E117C30
SHA-256:	143634615334FA1F670AA65AE0C494668FC5DFD52A36A46EFFB2D7EDAA187107
SHA-512:	E9BC02BC6C0FB766F514B26EADEF41045A9436214CA852F6207AD8633FB52B86DB19E8EC25A920940B996AEA774F47A3A9FD5E80201C35671B6D16A5CBEE7B9F
Malicious:	false
Preview:	...|B.~"QK%V..0...E*vnu..u.]<...`?)....#.G.....v.....{+.....s`..J.k...#...O..B.....\....<..8f.a.<^o.9Zch."...j.XoeC..h.!..H..|.....k..l..n..0'.....^o..._...^.;.~....+....;.U...&T~:...`..H.Q..CT.. +.Q4F.....L.. .%..._.A.y.....X"...P{.uM...c..k....p.. ..xV.&b2A>f....n.._..n.h/#..6....a.H6...p..n.e.fU.P,O...N.....+'G....g.Uu....D...*z.^..A.P..].F.E~.o....}..G..7L..S....s.r....4_D.. .....ibk..1&..F.W...X.....m3GEJ.Gzc..;..J"...[.....o.9..k.2!x.'S..}./=i..u.\X.I.....b(R/Y.a?...,.4_...^..-..FZ..7d.B.=.HY.....x....f(Sax....l..e..CR..f...LvL.3.:.x.v...._'..11.$mq...$. s,p=89..`.... ...L...'..i.....Z.O...f<..;qjM}.p(&...v^.....Ub.a5A..B.....$.....W`/2....p....Je.-...PF.-J.k:.0u.Kx~S'.>.....~. Z.q./.....I.]..~9&..j.,..S."..Y....aiY.6Or1.v..dV~."....h y..6!:<.G.....z.^..S.@.Z.pE.s#.+E.I..i.j..p..C..x.C...\.l.z.3".R..G`+...a.h....D!.4e....n....}.....z....0.}dV..<.`.....QMf5.O...J.%f.'Q... .$.Wj.Es..FLE...:..>.....*..].(

C:\Users\user\Desktop\GAOBCVIQIJ\EEGWXUHVUG.png	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978335496028412
Encrypted:	false
SSDEEP:	192:3dLy48vX6c8TqxVyZMjWQXrEeZUEG2wpM/g6ywfYFe53K0V+n:NL38vX6hT4/j7Xrz+Swpg1Doqm
MD5:	C9A28F36D717389FAE7C4426D78950F8
SHA1:	F19CE42DEEC132179CC560A0CFEB1785C8ECF70B
SHA-256:	1BC2F202F3883155505766DEBDB2B83A37EBE1D6FF3BDB03551D2ED960D187C6
SHA-512:	3F76B4FDDE8B7D8BCAB42572F3AC4EB49508EF70B1F7F4552B0E807E5B198C3AC4AAD12CCD29288C4735E30B94823C90EF8C602B6E64A2B63474967CAA80B6C
Malicious:	false
Preview:	.....FN.l_..L..P<..\@.!^o..5.one.s.[.....O..1.k....pf.A..o}....o .c"XxY.BR..-.`..iu.s....NgsnE.N...V.^.h..u....H.!,.7.c>*,D.i...-.C.f.QhVd.O..1.p...O...........Z.t....4...l^.....-.B..)..Qcp. w%4.Pv.......d...f.o2Qn.....r...d...P...K8(..#..[.......v]wv...6.l..!.W".YE4...b}... ...J.....r....@.2..A.\#.....j^.W.......Nt..QUF|..(0a ..|..S{c.MM.P. 9M.Z...C.......9.|/z.M.:c.w.3.v..>.t......<... ...DkL.H&.P^...9..V.Q........F.@]..'..75RP,-O.%.../..vu..x4!|.......J.....$X...*...?.....2.L....H.....I......../j.k..z.CLh.....TY.a.....d.E.....:.....>....<..../.;.}G...g..e...C$.C.Z...0n.`{.Y.$.w ..$..Y..1b2.W...E8b$...!!.@...K...'.g...../.....~..Q6.c.a.(.E.....\|..p.q..}..#j.....`B.G........Q...Jj..h... ...'u...K.^\|..K.....:C..A.X\|..x.j.....#.e..J.j."..Ky.....^.7..h.K9.5.7}.....R*la..:..... c.2..q..M".%.~.....C\.."V$bf..........5z.r.l..aH.Qm..mgY.[..4..j.d....>..*...T..gH../..l..im7.....y... ...@..p.n...5.....1.........#....(..`S|V....Alb..

C:\Users\user\Desktop\GAOBCVIQIJ\EEGWXUHVUG.png.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978335496028412
Encrypted:	false
SSDEEP:	192:3dLy48vX6c8TqxVyZMjWQXrEeZUEG2wpM/g6ywfYFe53K0V+n:NL38vX6hT4/j7Xrz+Swpg1Doqm
MD5:	C9A28F36D717389FAE7C4426D78950F8
SHA1:	F19CE42DEEC132179CC560A0CFEB1785C8ECF70B
SHA-256:	1BC2F202F3883155505766DEBDB2B83A37EBE1D6FF3BDB03551D2ED960D187C6
SHA-512:	3F76B4FDDE8B7D8BCAB42572F3AC4EB49508EF70B1F7F4552B0E807E5B198C3AC4AAD12CCD29288C4735E30B94823C90EF8C602B6E64A2B63474967CAA80B6C
Malicious:	false
Preview:	.....FN.l_..L..P<..\@.!^o..5.one.s.[.....O..1.k....pf.A..o}....o .c"XxY.BR..-.`..iu.s....NgsnE.N...V.^.h..u....H.!,.7.c>*,D.i...-.C.f.QhVd.O..1.p...O...........Z.t....4...l^.....-.B..)..Qcp. w%4.Pv.......d...f.o2Qn.....r...d...P...K8(..#..[.......v]wv...6.l..!.W".YE4...b}... ...J.....r....@.2..A.\#.....j^.W.......Nt..QUF|..(0a ..|..S{c.MM.P. 9M.Z...C.......9.|/z.M.:c.w.3.v..>.t......<... ...DkL.H&.P^...9..V.Q........F.@]..'..75RP,-O.%.../..vu..x4!|.......J.....$X...*...?.....2.L....H.....I......../j.k..z.CLh.....TY.a.....d.E.....:.....>....<..../.;.}G...g..e...C$.C.Z...0n.`{.Y.$.w ..$..Y..1b2.W...E8b$...!!.@...K...'.g...../.....~..Q6.c.a.(.E.....\|..p.q..}..#j.....`B.G........Q...Jj..h... ...'u...K.^\|..K.....:C..A.X\|..x.j.....#.e..J.j."..Ky.....^.7..h.K9.5.7}.....R*la..:..... c.2..q..M".%.~.....C\.."V$bf..........5z.r.l..aH.Qm..mgY.[..4..j.d....>..*...T..gH../..l..im7.....y... ...@..p.n...5.....1.........#....(..`S|V....Alb..

C:\Users\user\Desktop\GAOBCVIQIJ\EFOYFBOLXA.mp3	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.980830467973997
Encrypted:	false
SSDEEP:	192:eppMigRHIxjjA86PivzJQPz7hqIRe0xZh6McVuV+n:0pM95IW3Pezs7kMnC7
MD5:	F8BA46F9A80CF8A8F35E7218FA651F42
SHA1:	87CE8DC9DADBD630DF7EB78F4E71B5C027915988
SHA-256:	BF079E760365D2975E6DE609DA142983135F55E7103368901804529B01CFF673
SHA-512:	9625A71461B55854D3D30844AB3405151FF58D5DB56F176E05E0DBC8DC001C6B63F71B2BDE39FE4DA1FE71F89B1AADF116321AB7F9214C14BEE6394E9AEAA87D
Malicious:	false

C:\Users\user\Desktop\GAOBCVIQIJ\EFOYFBOLXA.mp3	
Preview:	Z...qG..~.....^T:f...H...^Li..8r&..A.....j.{h.0.\i..R*.eV...F....$.;...|K.7=E-.u....l].5j..T...3..bg...[X.C*f.n...P.^.y....i.....D..,0K%.....H$.I35....j..L....8..!..~...|m6i...P..C..h.!q.=7~NX... 1..)}.....P.%..w.d.:...o.....L.0..''I..uw.~{....w.M...Dy....''.hG6..o.....6...G.)..%.J...}p..Q.....oJx.q..B...0....._#b.<c<.....az..z.e^..P.3X2.7`c~jm..s...}.....'[.../K...Ep..e\.z...myhL. .Q...h}.J.^.....C.....w.''.'.r.J.q.....S....H.....nT8.6f,.S.y.ZSt....2c`m/...+....;...~p.{.....W'..-|%..rH..y&;.;{.....Kq..(..:.S<.SFL...'.....v.....eZ.....M.''.....0..s`.}.=..k4D..+t.).....; ..dxdakv.....$.).....{.....{9+F.3.d.e.....u..c.....7....I....-.QA@.y..#5;.C..n.hJ..u.....z8...6Z..v..F=...F...%...A=38[..=..V...R.B.`...,(@$*.W..n0... !.,.+.o.C.p...{^..h.0...!.n&.!. .v...4.T...&X..Zb.B.E.6..(.5..3..d...p.!U..u.''.4.D..|..I....j.@X..z....o@yX...0.2....:<'.....T..P.!...S.[...Q....NQ.....5.._[0.....TRO...%.''.....?.?NE:.

C:\Users\user\Desktop\GAOBCVIQIJ\EFOYFBOLXA.mp3.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.980830467973997
Encrypted:	false
SSDEEP:	192:eppMigRHIxjjA86PivzJQPz7hqIRe0xZh6McVuV+n:0pM95IW3Pezs7kMnC7
MD5:	F8BA46F9A80CF8A8F35E7218FA651F42
SHA1:	87CE8DC9DADBD630DF7EB78F4E71B5C027915988
SHA-256:	BF079E760365D2975E6DE609DA142983135F55E710336890180452 9B01CFF673
SHA-512:	9625A71461B55854D3D30844AB3405151FF58D5DB56F176E05E0DBC8DC001C6B63F71B2BDE39FE4DA1FE71F89B1AADF116321AB7F9214C14BEE6394E9AEAA87 D
Malicious:	false
Preview:	Z...qG..~.....^T:f...H...^Li..8r&..A.....j.{h.0.\i..R*.eV...F....$.;...|K.7=E-.u....l].5j..T...3..bg...[X.C*f.n...P.^.y....i.....D..,0K%.....H$.I35....j..L....8..!..~...|m6i...P..C..h.!q.=7~NX... 1..)}.....P.%..w.d.:...o.....L.0..''I..uw.~{....w.M...Dy....''.hG6..o.....6...G.)..%.J...}p..Q.....oJx.q..B...0....._#b.<c<.....az..z.e^..P.3X2.7`c~jm..s...}.....'[.../K...Ep..e\.z...myhL. .Q...h}.J.^.....C.....w.''.'.r.J.q.....S....H.....nT8.6f,.S.y.ZSt....2c`m/...+....;...~p.{.....W'..-|%..rH..y&;.;{.....Kq..(..:.S<.SFL...'.....v.....eZ.....M.''.....0..s`.}.=..k4D..+t.).....; ..dxdakv.....$.).....{.....{9+F.3.d.e.....u..c.....7....I....-.QA@.y..#5;.C..n.hJ..u.....z8...6Z..v..F=...F...%...A=38[..=..V...R.B.`...,(@$*.W..n0... !.,.+.o.C.p...{^..h.0...!.n&.!. .v...4.T...&X..Zb.B.E.6..(.5..3..d...p.!U..u.''.4.D..|..I....j.@X..z....o@yX...0.2....:<'.....T..P.!...S.[...Q....NQ.....5.._[0.....TRO...%.''.....?.?NE:.

C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977158935336416
Encrypted:	false
SSDEEP:	192:dzsqkcr3YwgloaN7nS+vBtu//M4YZqgWur1oU+cMjteq4eg7zmM1l4gjbsg/ffvA:VKvlj5nNu04YFDpoJxXGzmutj5/ff4
MD5:	A6CB7175C912634850C25A8FA2F9F2DE
SHA1:	0DD7E4574FEF7DF05E215F7F726A3DEB0D821DFE
SHA-256:	DC28F1D7D7124FF81C16D53942A43771A2C58F22061CD74885EEB6788AA63BF1
SHA-512:	7A806504E47B10B13C6390309D2BF610DB49DB3115C4F33CCD1FBA22244A4623B0700C19CC96C1E8FBEA8ADAE6DAC1EFD63783B3CA9B77A4262BA5B64865E9 5F
Malicious:	false
Preview:	..lU.m.XB.....rWh>W....cu.....n...P..m''.....G.....!o~.....n.....v.$...|.. .k.Mh.m..e...`.4.f.Elg\.I*.$L.n..g..TM#)..r...W.....`..!..EP.De%.%..6|).....`.5 .CCi.....%....0[..LA..O b ..1....Gk.^....X~u1&..V)F..wl.-{.Ns-.....1o.Y.K.4B.....SR..#..2V.....~...*...8...f;BY.H.y.<....7..t....9=s…Nl....g.aK?Q&z....*$Wt..<.jdFC.K..i..*.l....'.''.0Q(.....B+x..^..n ..i...s..E..I.$7&.[V.M.#.o..RuLF.{.^/...@....2.[.5..e..C..T...z..n.....v3.84}shV.....]....iJ.....@@O..i&.I;8.2..d{...[.(.....x...y.u..h..''.g[..G..lF*.?.G.S,,..%..O....b]S.P...Y.{.8.... ...Q...$.E..''...c.Ej.IQ9..!.lVq.j.R..@.X..}5.;...:`.H..?*z.bj.q...{.M..Kr.....;HT.j''.....n...1.9..W.3U!..?.(....6...f.Y7..A..Ox....{.,.-.....fg~M.....4Y...A.....^dt.:...xJ`v....d.E..y.Q..... s.j.''T.=P...8..$....y.....?...1.$Pfv...b:Y....2o.y...R'''=..... FK|..J...%.G..u..b...PZ{.../.....0.~le.o...w.....X..M.#eQ..:u....=...v.Z..N6..!....m..1*.g....s.a.....M[.q=(....k<`..

C:\Users\user\Desktop\GAOBCVIQIJ\GAOBCVIQIJ.docx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977158935336416
Encrypted:	false
SSDEEP:	192:dzsqkcr3YwgloaN7nS+vBtu//M4YZqgWur1oU+cMjteq4eg7zmM1l4gjbsg/ffvA:VKvlj5nNu04YFDpoJxXGzmutj5/ff4
MD5:	A6CB7175C912634850C25A8FA2F9F2DE
SHA1:	0DD7E4574FEF7DF05E215F7F726A3DEB0D821DFE
SHA-256:	DC28F1D7D7124FF81C16D53942A43771A2C58F22061CD74885EEB6788AA63BF1
SHA-512:	7A806504E47B10B13C6390309D2BF610DB49DB3115C4F33CCD1FBA22244A4623B0700C19CC96C1E8FBEA8ADAE6DAC1EFD63783B3CA9B77A4262BA5B64865E9 5F
Malicious:	false
Preview:	..lU.m.XB.....rWh>W....cu.....n...P..m''.....G.....!o~.....n.....v.$...|.. .k.Mh.m..e...`.4.f.Elg\.I*.$L.n..g..TM#)..r...W.....`..!..EP.De%.%..6|).....`.5 .CCi.....%....0[..LA..O b ..1....Gk.^....X~u1&..V)F..wl.-{.Ns-.....1o.Y.K.4B.....SR..#..2V.....~...*...8...f;BY.H.y.<....7..t....9=s…Nl....g.aK?Q&z....*$Wt..<.jdFC.K..i..*.l....'.''.0Q(.....B+x..^..n ..i...s..E..I.$7&.[V.M.#.o..RuLF.{.^/...@....2.[.5..e..C..T...z..n.....v3.84}shV.....]....iJ.....@@O..i&.I;8.2..d{...[.(.....x...y.u..h..''.g[..G..lF*.?.G.S,,..%..O....b]S.P...Y.{.8.... ...Q...$.E..''...c.Ej.IQ9..!.lVq.j.R..@.X..}5.;...:`.H..?*z.bj.q...{.M..Kr.....;HT.j''.....n...1.9..W.3U!..?.(....6...f.Y7..A..Ox....{.,.-.....fg~M.....4Y...A.....^dt.:...xJ`v....d.E..y.Q..... s.j.''T.=P...8..$....y.....?...1.$Pfv...b:Y....2o.y...R'''=..... FK|..J...%.G..u..b...PZ{.../.....0.~le.o...w.....X..M.#eQ..:u....=...v.Z..N6..!....m..1*.g....s.a.....M[.q=(....k<`..

C:\Users\user\Desktop\GAOBCVIQIJ\QCFWYSKMHA.xlsx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9762813311262475
Encrypted:	false
SSDEEP:	192:aEj1nxX9wZUTo3o3qj3WgI4dGKlpGyG4q9KZdL5V+n:aEZnxNwP46j3WgI1Sqo/q
MD5:	ACD1E08330F0F55B4C6A1553605CA23B
SHA1:	A26301AAB709489262E996BF153691B6AC619B9B
SHA-256:	E97D8E60BB698D7D45A5D2367730336E56A7EB5714D8F682A6CAAD7B8C40D404
SHA-512:	596030F457D215AD6A9887DBA654770B59965394D05D2F6DD0FC659A28E55CE5CF4EED5E4386C716A5A65364D6517F815DE9F20219BC9D600E9DD2797AA405D
Malicious:	false
Preview:	... 0T....(....|".8....]E..q...E#Nsb..`.K.....]....fw.....'i.....m.%.ey...k.KzM!f.:.....:..a...*`.6.U`....q.Xe..:_.....">w.^.9.....{..ogT...V.<.....d.. .1z,:...).I...!.r.Q.....B.E...z..n.C..).d.=...z...-&>..."."...?.Y.....G...W.9Ir_vL...GH....<s..B.....tG....<...[].Y.%..^....|..LX.....K-.....5Y9c`..k..%Ru..0.rh.~.Y..]..tx87....."&..^.....Q....:*,..".k..Bbq.N..5*L...Tz.....>..,H...V. ....S...z.....nu.c....eNNX.z.r4J.....h..S...>.....6..%+.Ug...F...-K0..#N...0Kz..Q.8...W.*.W.....G.>.../.{..q..ud.. r..n...f..{.D80..f.....o0.....":.:..<..>=UP.....>.w.i.....N..... ...<...? .W...[.H....O..Q...[..,.....v.+..C _?UO.uHqj..::/,.....k I.~nk.>-F.aUf..<B.....b.h...,d.>...`.2...D;,...H.....1 J.L..pCR.r...[...{...F.3<~....._X.PE.1(..r..(.O%.~.....@KJ..^./..>/S6&...g bM.b.@...*..a.f\.....G..,<.4...S..v..j....~Oh..NQ# .....C..@....7.N.7r...(.FS.o...9.].V....?Y..DC4|.,...%...:....C..DGH+.E}....9Se...~.2d.V..m.-..'...

C:\Users\user\Desktop\GAOBCVIQIJ\QCFWYSKMHA.xlsx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9762813311262475
Encrypted:	false
SSDEEP:	192:aEj1nxX9wZUTo3o3qj3WgI4dGKlpGyG4q9KZdL5V+n:aEZnxNwP46j3WgI1Sqo/q
MD5:	ACD1E08330F0F55B4C6A1553605CA23B
SHA1:	A26301AAB709489262E996BF153691B6AC619B9B
SHA-256:	E97D8E60BB698D7D45A5D2367730336E56A7EB5714D8F682A6CAAD7B8C40D404
SHA-512:	596030F457D215AD6A9887DBA654770B59965394D05D2F6DD0FC659A28E55CE5CF4EED5E4386C716A5A65364D6517F815DE9F20219BC9D600E9DD2797AA405D
Malicious:	false
Preview:	... 0T....(....|".8....]E..q...E#Nsb..`.K.....]....fw.....'i.....m.%.ey...k.KzM!f.:.....:..a...*`.6.U`....q.Xe..:_.....">w.^.9.....{..ogT...V.<.....d.. .1z,:...).I...!.r.Q.....B.E...z..n.C..).d.=...z...-&>..."."...?.Y.....G...W.9Ir_vL...GH....<s..B.....tG....<...[].Y.%..^....|..LX.....K-.....5Y9c`..k..%Ru..0.rh.~.Y..]..tx87....."&..^.....Q....:*,..".k..Bbq.N..5*L...Tz.....>..,H...V. ....S...z.....nu.c....eNNX.z.r4J.....h..S...>.....6..%+.Ug...F...-K0..#N...0Kz..Q.8...W.*.W.....G.>.../.{..q..ud.. r..n...f..{.D80..f.....o0.....":.:..<..>=UP.....>.w.i.....N..... ...<...? .W...[.H....O..Q...[..,.....v.+..C _?UO.uHqj..::/,.....k I.~nk.>-F.aUf..<B.....b.h...,d.>...`.2...D;,...H.....1 J.L..pCR.r...[...{...F.3<~....._X.PE.1(..r..(.O%.~.....@KJ..^./..>/S6&...g bM.b.@...*..a.f\.....G..,<.4...S..v..j....~Oh..NQ# .....C..@....7.N.7r...(.FS.o...9.].V....?Y..DC4|.,...%...:....C..DGH+.E}....9Se...~.2d.V..m.-..'...

C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.pdf	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978330090145761
Encrypted:	false
SSDEEP:	192:vijpo83leNhNMK4InRTvSvBanabdIxmaSp6rkw36aenC1SV+n:+oaw20n5R0zIrkw36tC1n
MD5:	322AADF19704F30D6C34E1306D999F7A
SHA1:	C21E12D241E367155C160442C326DC64605B2E92
SHA-256:	D9BE2336917E7F36FA8E269D90C60AF0341E289D95D24475E321DFDAC1DA4D5C
SHA-512:	6037EC13C7C42F6E98DBD1D3C2ACE6581837C9515C3CF017D6592C26A107E870FDC5AE80C25099863DCEB8D562B8A8418D44315394FD522D066105A14DD3D2
Malicious:	false
Preview:	.'}....B....&.U.U.....-.X&....".M.0...P..5.D.....8...Q.e..o.....,.$....Q..R...+R..$M.V....'3P}....7I~..C.Y..:...=Vyy..).--..a|.....-.\.\.7 ....r.>3._.]I.j...PH..w.p;H....f..k.I...+....B.XbF H.a...y.F.z).n.<p@..).rn.]Y.G*(..#M.ByT..Dk.R..L(h.....Z....;vN.AP...#..w.....^..q.. .K.-..2@.....\.].W....LB.@ ..[r.. 4.....M....'.v....<O+(&..uj.....8.#..-.v.P(...t!...f /3n.u.]p.y..F.4..o.Q;.....)..>..[P.6.....svg.S...w.+....N....0y`.....[...._/!.,f8M".u...T.....t...)...,2).^.y>FK.!v6&\.i..|]....+.....W..hA.!k.....y..+N.;*8f....!)....0ud...k....0.....s.i.r..)..g8.... f.....A6.m..%...< pbws...{.w..6s....n...b....n.+j..h.,..E..L..a...sF,.N4.. .X{..1K.\.....KW`.!..t.S...}K]q!8m.....a.FX..g.....7."P....O#.K.0.=..=._!~.^..&...9.q.F...z...-..p1.0..k.....Ih.....["....iE.]c..Q.5g....'JB...G..a...'...v....k.1c.....Zr`.0lJR7....,....D.F.[.x.....!..{.....$DW..p..C@...q....C.....$qI.NG.q3..~<VI. ....&R..... .-c.i..._.

C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.pdf.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978330090145761
Encrypted:	false
SSDEEP:	192:vijpo83leNhNMK4InRTvSvBanabdIxmaSp6rkw36aenC1SV+n:+oaw20n5R0zIrkw36tC1n
MD5:	322AADF19704F30D6C34E1306D999F7A
SHA1:	C21E12D241E367155C160442C326DC64605B2E92

C:\Users\user\Desktop\GAOBCVIQIJ\SUAVTZKNFL.pdf.bCcBDeabea (copy)

SHA-256:	D9BE2336917E7F36FA8E269D90C60AF0341E289D95D24475E321DFDAC1DA4D5C
SHA-512:	6037EC13C7C42F6E98DBD1D3C2ACE6581837C9515C3CF017D6592C26A107E870FDC5AE80C25099863DCEB8D562B8A8418D44315394FD522D066105A14DD3D2
Malicious:	false
Preview:	.'}....B....&.U.U.....-.X&....".M.0...P..5.D.....8...Q.e..o....,..$....Q..R...+R..$M.V....'3P}....7I~..C.Y..:...=Vyy..).--..a|.....-.\.\.7 ....r.>3._.]I.j...PH..w.p;H....f..k.I...+....B.XbF H.a...y.F.z).n.<p@..).rn.]Y.G*(..#M.ByT..Dk.R..L(h.....Z....;vN.AP...#..w.....^..q.. .K.-..2@.....\.].W....LB.@ ..[r.. 4.....M....'.v....<O+(&..uj.....8.#..-.v.P(...t!...f /3n.u.]p.y..F.4..o.Q;.....)..>..[P.6.....svg.S...w.+....N....0y`.....[..._./!.,f8M".u...T.....t...)...,2).^.y>FK.!v6&\.i..|]....+.....W..hA.!k.....y..+N.;*8f....!)....0ud...k....0.....s.i.r..)..g8.... f.....A6.m..%...< pbws...{.w..6s....n...b....n.+j..h.,..E..L..a...sF,.N4.. .X{..1K.\.....KW`.!..t.S...}K]q!8m.....a.FX..g.....7."P....O#.K.0.=..=._!~.^..&...9.q.F...z...-..p1.0..k.....Ih.....["....iE.]c..Q.5g....'JB...G..a....'...v....k.1c.....Zr`.0lJR7....,.....D.F.[.x.....!..{.....$DW..p..C@...q....C.....$qI.NG.q3..~<VI. ....&R..... .-c.i.._.

C:\Users\user\Desktop\GAOBCVIQIJ\uCLrcwQ_readme_.txt

Process:	C:\Users\user\Desktop\ab.exe
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	3758
Entropy (8bit):	5.730064789432486
Encrypted:	false
SSDEEP:	48:L9k0ZzV7L/vNbXGZULVDgUp4qNiiE6bm1c0rfWejhAe/YAliM3PXnLHrYxgkH69e:L95zhLNbXGZUe7Ka6pU6i9fLrvE69USC
MD5:	41F60F7F111C974C7727BBFA483C63C2
SHA1:	18587F9751EAAE7C5C779A9BE2FF619CD2625C11
SHA-256:	9C9D056AC514D49FFAD38C17ADDCCD3DFC4C55132C944DDF76A4BB08A4137D51
SHA-512:	AC7F11B160C98750B14C4AF6926A02BBC4D42C17BD9A44316DF861CA7BA94BB3FA8C956794C63049F64B341D3EFFCD24601533250633D8BEA585221082D3C1C
Malicious:	false
Preview:	-------=== Your network has been infected! ===-------.....********** DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED ********** .....All your documents, photos, databases and other important files have been encrypted and have the extension: .bCcBDeabea.....You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!.....The only way to restore your files is to buy our special software. Only we can give you this software and only we can restore your files!.....We have also downloaded a lot of private data from your network....If you do not contact as in a 3 days we will post information about your breach on our public news website (avaddongun7rngel.onion) and after 7 days the whole downloaded info.....You can get more information on our page, which is located in a Tor hidden network.....How to get to our page...----------

C:\Users\user\Desktop\LSBIHQFDVT.docx

Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.98012572202099
Encrypted:	false
SSDEEP:	192:hKs+JKiO/BAwuyYdcK4EQ2TDWgusQUs0p7QrFp9IqKCb/rPqV+n:hJ/H3YrhvTRusbs0pI9nZXP
MD5:	739539EBC633007778F01BF49AB86DA3
SHA1:	8C5E0628C38BC14C548F2759B7185B6E899BC8D9
SHA-256:	66C629C5A5E4313B71F31C079E8D69BE02348EE78C5CB80EBF96C913B1D7024F
SHA-512:	E0D2E88608B324DAA050E575F0EE4861D9F257915A8F79C42230A3DD7483A6DAF53BFC2F4FBD98F697E819AEB11E683655571A3147E5709E2B36BFF1D3D6609A
Malicious:	false
Preview:	....5Bf.&.....I./...u...L1.|....A...:;..I^.7e.38$"..~....2.!Y...w?).f..Ut.1....d78....B..].b..e;..iA."D..d.h.\|u.b"$.. ...I..x.I.5.n7QkhE./h..k.n0h..2*6..M^fF&...(.....]9....a....K.z..PrA[3..... ....|@...d@..3...z..#}L.....K.....gHR..o+..[.....-.n...{.....tp8n...YI.u.3S.s.'y.d".i.`.b.0.Y.h2.=.....u.22L..a..Z..cu)P.P..rK.$.(.?.k.....H.V.w.....i.....o^{...-.~.G._.SG3H.-.....X '..f%.....lj.UW...;.....[j...d...M2J...T..,..Wf...X...,.uEK..'^.,.7z.P...{.}.p..LH..o.....^..A\|....Th....G..+.B..G..).....fq.....\|Vbs>v.y.%.....Y..&&...%.WA....{.,.;..UTJ[..gW.4{.E.\.p..d.. S:.#Q..[..s....QY....'w.I{....g...z.....F.=.r.F.f..~o.0g.K..r..e`....e....x!.m....o.i&fm.H.W~w.$}L7Lx.H..l.B%...._.N.....s..)..gf.R...yj.%.....7..c....9.....?c..._V@..v-Gr..CA....E....z...Aw.. {..'O.....z...d?0y..#O..(..e...}.8..=...8..&Zv.N.o.\.n.....`..K....r...};'k.n._..E....!..4C..<...7bEN".7.....%.%..nA#..1.}1.+w...Z..2VN.....|...#M.+9..w

C:\Users\user\Desktop\LSBIHQFDVT.docx.bCcBDeabea (copy)

Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.98012572202099
Encrypted:	false
SSDEEP:	192:hKs+JKiO/BAwuyYdcK4EQ2TDWgusQUs0p7QrFp9IqKCb/rPqV+n:hJ/H3YrhvTRusbs0pI9nZXP
MD5:	739539EBC633007778F01BF49AB86DA3
SHA1:	8C5E0628C38BC14C548F2759B7185B6E899BC8D9
SHA-256:	66C629C5A5E4313B71F31C079E8D69BE02348EE78C5CB80EBF96C913B1D7024F
SHA-512:	E0D2E88608B324DAA050E575F0EE4861D9F257915A8F79C42230A3DD7483A6DAF53BFC2F4FBD98F697E819AEB11E683655571A3147E5709E2B36BFF1D3D6609A
Malicious:	false

C:\Users\user\Desktop\LSBIHQFDVT.docx.bCcBDeabea (copy)	
Preview:	....5Bf.&.....I./...u...L1.|....A...:.;..I^.7e.38$"..~....2.!Y...w?).f..Ut.1....d78....B..].b..e;..iA."D..d.h.|u.b"$.. ...I..x.I.5.n7QkhE./h..k.n0h..2*6..M^fF&...(.....]9....a....K.z..PrA[3..... ....|@...d@..3...z..#}L.....K.....gHR..o+..[.....-.n...{.....tp8n...YI.u.3S.s.'y.d".i.`.b.0.Y.h2.=.....u.22L..a..Z..cu)P.P..rK.$.(.?.k.....H.V.w.....i.....o^{...-.~.G._.SG3H.-.....X '..f%.....lj.UW...;.....[j...d...M2J...T..,..Wf...X...,.uEK..'^.,.7z.P...{.}.p..LH..o.....^..A\|....Th....G..+.B..G..).....fq.....\|Vbs>v.y.%.....Y..&&...%.WA....{.,.;..UTJ[..gW.4{.E.\.p..d.. S:.#Q..[..s....QY....'w.l{....g...z.....F.=.r.F.f..~o.0g.K..r..e`....e....x!.m....o.i&fm.H.W~w.$}L7Lx.H..l.B%...._.N.....s..)..gf.R...yj.%.....7..c....9.....?c..._V@..v-Gr..CA....E....z...Aw.. {.."O.....z...d?0y..#O..(..e...}.8..=...8..&Zv.N.o.\.n.....`.K....r...};'k.n._..E....!..4C..<...7bEN".7.....%.%..nA#..1.}1.+w...Z..2VN.....|...#M.+9..w

C:\Users\user\Desktop\LSBIHQFDVT\GAOBCVIQIJ.pdf	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977759643434391
Encrypted:	false
SSDEEP:	192:KvSX/nSnUW8C1RaELeOObCwJg2GlaRQu1EuZNWWqqYkQujxe+InCUV+n:V+HfRJ6DJJgflaRQuqufaquujE+6CF
MD5:	566F47657935E7EC6EAA7E780573DBED
SHA1:	A0500C4C040ACD6BFED5B8068BC991F6B69D75E3
SHA-256:	D691942ED928C974C10BCD4402FBA1F6023A836648E8A660F9D6E74812B74002
SHA-512:	2DF146053D06CDE9238C9630772084C8B5E7BE96162C0BC3508A1313F2D4DD38A4FD031C90F4207A8AFCE3FF59FDAF93591CA53EFC3AFA9A696231E2B77ACA 2
Malicious:	false
Preview:	......a.G..-.....G.Fs.K~X~.|..N...j..... ...SZ:.^0.)D...D..D....(..H.?m.....?..;'G.....>bc.,.T.z.*...6....NQ...[C...xT.%....w.....y..Y..._.Z.=|\.....$1.....n.r...>.;...I...M.,.n.....q.c... h...]...A...c.58r^...N.....P...I....M..l.V.QI....,..._....r.....&....j.`.v...r..Yg...vIv..^.j..*...N.....q.\|.0.....!..D\.H....>iZ....o....'...8I.k.$.v.\..U..>...yU..v...:9.t.>.B....s.'Yq....5.B(..6.e. .bL....G.WBlh=..5.....r}..Xp....k...,. .[L...W.g.....*%....L S0....E.%S.....[/..*r.y.A.o//.....2.....rS...{.....U....x.....j>P'....|....g$b._...r/.E...&g...m..;u.;.z...P...N.[Dl...U. ..\|. .#;....M-....u;....W..A.y.rL`.m.Za...S9..<.!X..YB..."....w.f.<C.....*..(^4y.n.9..r,..G....xW...6B8Qc.pzc.....0ef.....cUU..s...nP...uCD...t)sT..5.n..;.....l*..f...z..)G)./.9.~.D....d..- ...Q.'KK.'%.a....<..c...F7.]..[.X5..T..f..Q>..e...pi.p"....S<=....'*E.L.....]..+a.Y]&.)..1...@&....?....4.!....).A....!.D ..`@..w$...

C:\Users\user\Desktop\LSBIHQFDVT\GAOBCVIQIJ.pdf.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977759643434391
Encrypted:	false
SSDEEP:	192:KvSX/nSnUW8C1RaELeOObCwJg2GlaRQu1EuZNWWqqYkQujxe+InCUV+n:V+HfRJ6DJJgflaRQuqufaquujE+6CF
MD5:	566F47657935E7EC6EAA7E780573DBED
SHA1:	A0500C4C040ACD6BFED5B8068BC991F6B69D75E3
SHA-256:	D691942ED928C974C10BCD4402FBA1F6023A836648E8A660F9D6E74812B74002
SHA-512:	2DF146053D06CDE9238C9630772084C8B5E7BE96162C0BC3508A1313F2D4DD38A4FD031C90F4207A8AFCE3FF59FDAF93591CA53EFC3AFA9A696231E2B77ACA 2
Malicious:	false
Preview:	......a.G..-.....G.Fs.K~X~.|..N...j..... ...SZ:.^0.)D...D..D....(..H.?m.....?..;'G.....>bc.,.T.z.*...6....NQ...[C...xT.%....w.....y..Y..._.Z.=|\.....$1.....n.r...>.;...I...M.,.n.....q.c... h...]...A...c.58r^...N.....P...I....M..l.V.QI....,..._....r.....&....j.`.v...r..Yg...vIv..^.j..*...N.....q.\|.0.....!..D\.H....>iZ....o....'...8I.k.$.v.\..U..>...yU..v...:9.t.>.B....s.'Yq....5.B(..6.e. .bL....G.WBlh=..5.....r}..Xp....k...,. .[L...W.g.....*%....L S0....E.%S.....[/..*r.y.A.o//.....2.....rS...{.....U....x.....j>P'....|....g$b._...r/.E...&g...m..;u.;.z...P...N.[Dl...U. ..\|. .#;....M-....u;....W..A.y.rL`.m.Za...S9..<.!X..YB..."....w.f.<C.....*..(^4y.n.9..r,..G....xW...6B8Qc.pzc.....0ef.....cUU..s...nP...uCD...t)sT..5.n..;.....l*..f...z..)G)./.9.~.D....d..- ...Q.'KK.'%.a....<..c...F7.]..[.X5..T..f..Q>..e...pi.p"....S<=....'*E.L.....]..+a.Y]&.)..1...@&....?....4.!....).A....!.D ..`@..w$...

C:\Users\user\Desktop\LSBIHQFDVT\LSBIHQFDVT.docx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.982073770414174
Encrypted:	false
SSDEEP:	192:+snS+fRzILRt9YdRfnAMgxdt589GpyxNVOEpgJHMMRaDP4QwThV+n:+wRJMLP9otgdG0I7EEGJHMhDAN+
MD5:	5EC97A3E7E0D953E1C1F8F22150C2A35
SHA1:	804139297A367617AA27AE73B68CA49D81613965
SHA-256:	A1B9C8E42CC60E5BEE088283CEFC38E4DFBABA1C5E11C7122DFADC98E0BC1E14
SHA-512:	A830FB2A2DAFFD9AB9F6A7A19455F1122A47B1165662735DB6CD984C085D8AAF730D481BDBAD0AFCB7523338A3D8B3FD6DBD24B2257CE3634FBBFBC562BDA AA1
Malicious:	false
Preview:	....W.)Hk...:;..~.|.I;.2qeK(m,....q...V.o..g.~.i...C...&.O@9....Hvn.P..vSdUF.W..$....R...c.7!..7.?...Q.cl.....>...-....Em...r3..NxG.A...`....$...pb.b.`.....x.U...t....n..kjHO.....Z.....v$ ...U<O.!..SI....:G.H].).M....W.p..o) .B...9..G..6a....i.GeB"bi.....k.....+(xa.....f..9.][.K.s...O6.kI.A{p...HE~...'$.?..t..[.}.'.s'u.....:....G.^..4.6*.y..g.a.....]..VH.6...h`<.....$. .k.#....d'..|.....{N....^7".n..`=Yn..rB,...G...i.= .L6.=~.%k..L....k.n....=.3...[....X}..Q,.?...p.R..I.6..{}I..)4t'...QJ4..9.....e.O?.5.. ...&.....`...V.|.....-..M@8..*..q..S.]9.o..j.l_.9a..k/.j. lb..:s.=..r.E..-.%[y..9.(2..<..5.l...../>g.c..[@..@.<.,.Y.....J])?....Z...Vy1..^>.>T$n.C..O....&..1..".D&tyf.....w).n...(A..u.@2..;J=.0db.,....b.M.....b..+ak.@m...:...+'"Z.oF.N\.b[_ .r69=/J...`2VQn..h[i'..^2..M..^i..'8..e;n.@|D.e.2|..{..Q..a-.`..%.Z..)'^`.>B#b\....7....ffb.....d.+.....}.../..&...Q.-....=...@.W0...Q...>.w?~.;.9...Zs.?=.o...dH..f

C:\Users\user\Desktop\LSBIHQFDVT\LSBIHQFDVT.docx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.982073770414174
Encrypted:	false
SSDEEP:	192:+snS+fRzILRt9YdRfnAMgxdt589GpyxNVOEpgJHMMRaDP4QwThV+n:+wRJMLP9otgdG0I7EEGJHMhDAN+
MD5:	5EC97A3E7E0D953E1C1F8F22150C2A35
SHA1:	804139297A367617AA27AE73B68CA49D81613965
SHA-256:	A1B9C8E42CC60E5BEE088283CEFC38E4DFBABA1C5E11C7122DFADC98E0BC1E14
SHA-512:	A830FB2A2DAFFD9AB9F6A7A19455F1122A47B1165662735DB6CD984C085D8AAF730D481BDBAD0AFCB7523338A3D8B3FD6DBD24B2257CE3634FBBFBC562BDAAA1
Malicious:	false
Preview:	....W.)Hk...:;..~.|.I;.2qeK(m,....q...V.o..g.~.i...C...&.O@9....Hvn.P..vSdUF.W..$....R...c.7!..7.?...Q.cl.....>...-....Em...r3..NxG.A...`....$...pb.b.`.....x.U...t....n..kjHO.....Z.....v$ ...U<O.!..SI....:G.H].).M....W.p..o) .B...9..G..6a....i.GeB"bi.....k.....+(xa.....f..9.][.K.s...O6.kI.A{p...HE~...'$.?..t..[.}.'.s'u.....:....G.^..4.6*.y..g.a.....]..VH.6...h`<.....$. .k.#....d'..|.....{N....^7".n..`=Yn..rB,...G...i.= .L6.=~.%k..L....k.n....=.3...[....X}..Q,.?...p.R..l.6..[}I..)4t'...QJ4..9.....e.O?.5... ...&.....`...V.|.....-..M@8..*..q..S.]9.o..j.l_.9a..k/.j. lb..:s.=..r.E..-.%[y..9.(2..<..5.l...../>g.c..[@..@.<.,.Y.....J])?....Z...Vy1..^>.>T$n.C..O....&..1..".D&tyf.....w).n...(A..u.@2..;J=.0db.,....b.M.....b..+ak.@m...:...+'"Z.oF.N\.b[_ .r69=/J...`2VQn..h[i'..^2..M..^i..'8..e;n.@|D.e.2|..{..Q..a-.`..%.Z..)'^`.>B#b\....7....ffb.....d.+.....}.../..&...Q.-....=...@.W0...Q...>.w?~.;.9...Zs.?=.o...dH..f

C:\Users\user\Desktop\LSBIHQFDVT\PWCCAWLGRE.mp3	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.980014852290303
Encrypted:	false
SSDEEP:	192:2TaJO0KUgFyXJSWyDw3rxlIDTbskzmZJC4Be5mxRNlwNargOn4fV+n:2WJ9xNyw7bIDXskzm+4Y5MNlwgsOn4I
MD5:	C399C6ED9CFC02A25FF1550CAA31B8CE
SHA1:	3AD30F5B51A29B51BAC7562582DB1C1E2A81FDFD
SHA-256:	666D944652028581FC5DFEAFACBAD7F796B2B22CB29516667C69BF0F00616624
SHA-512:	85E2C998D880AFC9213528319185E26C17B3AAF3B2B4CCBDF7C535C9EA6E7905735E7430594B96096C027918BE434329422BE55ED346F284E15DA5142CD2429A
Malicious:	false
Preview:	....~P..S.x....!.M.a.`....g....]CF+d...b..}.L.....c(.~....3.?... .I.W}.x..rpxW.... ...Y...'.A.'...S...I../...G.{.....,y.....].)D..c.g.9.F....Q......C..),.iB...5..O.P...;Pp..=........{.C....z (....%..t....LzT.. |)v<.....Fo....5........|.......m4&.....o....\..+x ZM./........p..z....M.{...-...#.k1...4..#...N.D.Q..qZln..9..t.T....B..}..~OL.w......p.e^.......Eg...d..TU..:[u......f7M,.w+Q........H{.c....;"..)=.].6 ....>..DqGM.!..od.b..a.F...g[.$.GYT...z.dG*..P}.m{&ji9.8=.+..z7q.L*+..G....P]...G..}bs...F.{FM5-.*....r....g.\|.a..6....o=.....m..S..q.Y&.1....{.......L..+..?.*.0..\..<}......^MRg.~oh,..*.. Q....^..<...?.g\..K.W._t.$F..".>.>W8".3$.a..9n...ZvG.h.Ls..A....iN..."..P._VN./....z=c.$mm...@...6:.!.1...:.F.....:.../..H{f..5....F...n.3.E0..CJ..]....2,....y.. ../.....+...Q==}....>.... ..6.]?...`.X.."..).../....."..H.....T7..]("..Tz.\L.j.K...W0.....[Y.....P.q|9..Q..W.S...tm...$.P.N..I..\..:.,.q....x.I.....%....e.Q)J~ .7

C:\Users\user\Desktop\LSBIHQFDVT\PWCCAWLGRE.mp3.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.980014852290303
Encrypted:	false
SSDEEP:	192:2TaJO0KUgFyXJSWyDw3rxlIDTbskzmZJC4Be5mxRNlwNargOn4fV+n:2WJ9xNyw7bIDXskzm+4Y5MNlwgsOn4I
MD5:	C399C6ED9CFC02A25FF1550CAA31B8CE
SHA1:	3AD30F5B51A29B51BAC7562582DB1C1E2A81FDFD
SHA-256:	666D944652028581FC5DFEAFACBAD7F796B2B22CB29516667C69BF0F00616624
SHA-512:	85E2C998D880AFC9213528319185E26C17B3AAF3B2B4CCBDF7C535C9EA6E7905735E7430594B96096C027918BE434329422BE55ED346F284E15DA5142CD2429A
Malicious:	false
Preview:	....~P..S.x....!.M.a.`....g....]CF+d...b..}.L.....c(.~....3.?... .I.W}.x..rpxW.... ...Y...'.A.'...S...I../...G.{.....,y.....].)D..c.g.9.F....Q......C..),.iB...5..O.P...;Pp..=........{.C....z (....%..t....LzT.. |)v<.....Fo....5........|.......m4&.....o....\..+x ZM./........p..z....M.{...-...#.k1...4..#...N.D.Q..qZln..9..t.T....B..}..~OL.w......p.e^.......Eg...d..TU..:[u......f7M,.w+Q........H{.c....;"..)=.].6 ....>..DqGM.!..od.b..a.F...g[.$.GYT...z.dG*..P}.m{&ji9.8=.+..z7q.L*+..G....P]...G..}bs...F.{FM5-.*....r....g.\|.a..6....o=.....m..S..q.Y&.1....{.......L..+..?.*.0..\..<}......^MRg.~oh,..*.. Q....^..<...?.g\..K.W._t.$F..".>.>W8".3$.a..9n...ZvG.h.Ls..A....iN..."..P._VN./....z=c.$mm...@...6:.!.1...:.F.....:.../..H{f..5....F...n.3.E0..CJ..]....2,....y.. ../.....+...Q==}....>.... ..6.]?...`.X.."..).../....."..H.....T7..]("..Tz.\L.j.K...W0.....[Y.....P.q|9..Q..W.S...tm...$.P.N..I..\..:.,.q....x.I.....%....e.Q)J~ .7

C:\Users\user\Desktop\LSBIHQFDVT\QCFWYSKMHA.png	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.979869139483104
Encrypted:	false
SSDEEP:	192:S/MgHFtWhobuXqMLkl4jjBcCCiGulkuvNJ3DXNoD2faJV+n:SEgHFCob/4kMjBcCbGul9J3SWaW
MD5:	A01805CBA96EEA193DD185B472AB0687

C:\Users\user\Desktop\LSBIHQFDVT\QCFWYSKMHA.png	
SHA1:	F2EBB66D34AD7C4B16A0E306A62B7A9D29993920
SHA-256:	00F05D157EC5F6088A21EACFD09503010F8250D1A35B1C90FFF592FDEA3DA951
SHA-512:	5B30ED7D037C772F8C1ECB42CC18BC22AB4715916D9823666B4D244DAA94C130FA784BC669D98972987846CE55A3766650206AD5C6226384C95E3591F0C79E8(
Malicious:	false
Preview:	._..Q\..hq+>.KU../^N.. ..<Kgux.4I3...Q%.J.y..R.....q1....K ...2..a._.3X.C`....W.........O....:.!.9..".'R0.".$7...H..YFI.6sh........b.<....r3[...t?;..........%.s.V.^..@`.........6..''*q}DxtQ.y .0.:.....Q........[.s...|.#.....Kl..V.=..LnvyD.M.......Fl..m..Y..../...q.5L.X-..b.l....(..h..p.=.r..... ....vA.S.....'.QZ^....._.w.p1..o.!...M.e.....2..PTu....PF..A.....+>.....C\|BWi.5''..n...a.I.. ..6.C+..4..-R~%.Iq..:.k.*.fc./... S.'0~.F..}.L!.S]z....{.U.....I.R._.....-..k2.$.:}.....I..N.-MH.W....+....}L...OY..e...........mk.-...O|...f.....R./.......E. ...o.....~....E5.....m...!O.. ..X.........P... <8.....r...6S.^....5.k-_jn.#0..W..^....Z.K..8].*...>.c..#(..g.'.n..tQ*.[.....!..4.hQ?/....#..y'..Oh.....g.....gXC...n...G.......b..v,.T...`=Zr...a~...b..~.$KL.....w.'_.....'u.kj]!.2...N....G>F.|,.. .L.a....)..c.V!zS+.....n.....ir8.M...7.n.x.Xj.o..X..3..<e.v...A. ....iJ.~.....{..;.q..Nq.(1rGm.&.64...^.m.....T6A.....N.:..H..DC..

C:\Users\user\Desktop\LSBIHQFDVT\QCFWYSKMHA.png.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.979869139483104
Encrypted:	false
SSDEEP:	192:S/MgHFtWhobuXqMLkl4jjBcCCiGulkuvNJ3DXNoD2faJV+n:SEgHFCob/4kMjBcCbGul9J3SWaW
MD5:	A01805CBA96EEA193DD185B472AB0687
SHA1:	F2EBB66D34AD7C4B16A0E306A62B7A9D29993920
SHA-256:	00F05D157EC5F6088A21EACFD09503010F8250D1A35B1C90FFF592FDEA3DA951
SHA-512:	5B30ED7D037C772F8C1ECB42CC18BC22AB4715916D9823666B4D244DAA94C130FA784BC669D98972987846CE55A3766650206AD5C6226384C95E3591F0C79E8(
Malicious:	false
Preview:	._..Q\..hq+>.KU../^N.. ..<Kgux.4I3...Q%.J.y..R.....q1....K ...2..a._.3X.C`....W.........O....:.!.9..".'R0.".$7...H..YFI.6sh........b.<....r3[...t?;..........%.s.V.^..@`.........6..''*q}DxtQ.y .0.:.....Q........[.s...|.#.....Kl..V.=..LnvyD.M.......Fl..m..Y..../...q.5L.X-..b.l....(..h..p.=.r..... ....vA.S.....'.QZ^....._.w.p1..o.!...M.e.....2..PTu....PF..A.....+>.....C\|BWi.5''..n...a.I.. ..6.C+..4..-R~%.Iq..:.k.*.fc./... S.'0~.F..}.L!.S]z....{.U.....I.R._.....-..k2.$.:}.....I..N.-MH.W....+....}L...OY..e...........mk.-...O|...f.....R./.......E. ...o.....~....E5.....m...!O.. ..X.........P... <8.....r...6S.^....5.k-_jn.#0..W..^....Z.K..8].*...>.c..#(..g.'.n..tQ*.[.....!..4.hQ?/....#..y'..Oh.....g.....gXC...n...G.......b..v,.T...`=Zr...a~...b..~.$KL.....w.'_.....'u.kj]!.2...N....G>F.|,.. .L.a....)..c.V!zS+.....n.....ir8.M...7.n.x.Xj.o..X..3..<e.v...A. ....iJ.~.....{..;.q..Nq.(1rGm.&.64...^.m.....T6A.....N.:..H..DC..

C:\Users\user\Desktop\LSBIHQFDVT\QNCYCDFlJJ.jpg	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976243017495167
Encrypted:	false
SSDEEP:	192:H3tO90IFcemEsETYhqGZwaUA67YqXEz4FmaCTNbDV+n:W0xem/1ZUo8TFlCBb0
MD5:	45C14B3608A85F81FDB9826258B3A2EF
SHA1:	6EC31E06CE0D4E5788FF3C06C8FE0680C4883DB1
SHA-256:	D05C6A4EBEAFDCC076CD3F15FD0588D2F51917BEE7936383F846F6F4D5C4C5D4
SHA-512:	9D4B75874A91717265EEDB5B13015A23B8FA39B4C5E0A015AC08DE56AA7C0F062EDC76748C873793F83509F07839AD6E0FFC3DBAC70BF080F04D148D84CB4A6 E
Malicious:	false
Preview:	.q....aX....o.rfv^..G.z...m.....S.(.-.M.V....4.I..X...V...c.2.?....]..M...vn).....&_.b0....:.KJ.r.....2....oc.fu.....NP.(..e."...W..H....~..;.Nx.B...P...".[.NM.+j..R...f..r7+./)K.L.S. .;.O.z.j..>..7.Nni.6.~...>8.%..s.aQ.....D.=..nR~....rp.....U.....3...r5;.'..V\..!Q..*5.0>>E.....g.V.+.hl'..V.<..~sSQ.c.^...fs4+.R7'.....y~;T.;.._.l.>..r(...2r.\C}.'D..=y...S.[.,L[.1..4YJ .wm..''.....A.5.G]...z>.R...'.O....%...^.'A.D*^A.....\S..e...M8..p...M.=.._..z...q...A..5. /Iq.BN.N.....N.a..e\..G..:e..~....JW.....f.Z|<P....4l..rV...>>...&.~..9=....&...=..wLZVG..6j,S .W"R..S..@.K9.-....}2n$..f#...H.-Cp.g.....<].YSi...F..jt.K.A.>..khe./X...<.fc.,.X....]!.0....L.....M..C@...0.X.#x#u.3.CA.....9..X.B.1..6L.LR<...^.....H,d.....7....1.Hn.x.!.+..v..>....-. X..w.D.els..y..%..)|.8.,....x..%.9..q+..O..F`R.u...w[.rt.....Q.bzc.jU..^[J.-.-.I..l.'.<..~;%.w..0.5....1-.Y.....).W..s....9.~.V...C.....'j....q...)G-.....v.....+...

C:\Users\user\Desktop\LSBIHQFDVT\QNCYCDFlJJ.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976243017495167
Encrypted:	false
SSDEEP:	192:H3tO90IFcemEsETYhqGZwaUA67YqXEz4FmaCTNbDV+n:W0xem/1ZUo8TFlCBb0
MD5:	45C14B3608A85F81FDB9826258B3A2EF
SHA1:	6EC31E06CE0D4E5788FF3C06C8FE0680C4883DB1
SHA-256:	D05C6A4EBEAFDCC076CD3F15FD0588D2F51917BEE7936383F846F6F4D5C4C5D4
SHA-512:	9D4B75874A91717265EEDB5B13015A23B8FA39B4C5E0A015AC08DE56AA7C0F062EDC76748C873793F83509F07839AD6E0FFC3DBAC70BF080F04D148D84CB4A6 E
Malicious:	false

C:\Users\user\Desktop\LSBIHQFDVT\QNCYCDFlJJ.jpg.bCcBDeabea (copy)	
Preview:	.q....aX....o.rfv^..G.z...m.....S.(.-.M.V....4.I..X...V...c.2.?....]..M...vn).....&_.b0....:.KJ.r.....2....oc.fu.....NP.(..e."...W..H....~.;.Nx.B...P..."..[.NM.+j..R...f..r7+./)K.L.S. .;.O.z.j..>..7.Nni.6.~...>8.%..s.aQ.....D.=..nR~....rp.....U.....3...r5;'..V\..!Q..*5.0>>E.....g.V.+.hl'..V.<..~sSQ.c.^...fs4+.R7'.....y~;T.;.._.I.>..r(...2r.\C}.'D..=y...S.[.,L[.1..4YJ .wm..".....A.5.G]...z>.R...'.O....%...^.'A.D*^A.....\S..e...M8..p...M.=.._..z...q...A..5. /Iq.BN.N.....N.a..e\..G..:e..~....JW.....f.Z|<P....4l..rV...>>...&.~..9=....&...=..wLZVG..6j,S .W"R..S..@.K9.-....}2n$..f#...H.-Cp.g.....<].YSi...F..jt.K.A.>..khe./X...<.fc.,.X....]!.0....L.....M..C@...0.X.#x#u.3.CA.....9..X.B.1..6L.LR<...^.....H,d.....7....1.Hn.x.!.+..v..>....-. X..w.D.els..y..%..)|.8.,....x..%.9..q+..O..F`R.u...w[.rt.....Q.bzc.jU..^[J.-.-..I..I.'.<..~;%.w..0.5....1-.Y.....).W..s....9.~.V...C.....'j....q...)G-.....v.....+...

C:\Users\user\Desktop\LSBIHQFDVT\ZQIXMVQGAH.xlsx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.979914364379438
Encrypted:	false
SSDEEP:	192:65doJBeuD/TEEaWMOVPkCmE9Gy4sY/SIMvlgV+n:moHeuD7EEWUPdzwSIMNZ
MD5:	2FB1513EDEFA0C8EF8AE7C8AB410049F
SHA1:	3AFF715E3EDFCBEE3801A6D81088875B2E941C9C
SHA-256:	DDDE7183DA60E6526499CDF42FBEA175FCCC2DC61B64A59DD94E08D0B0DDC8F2
SHA-512:	0E6C46B7457C5472120757FABDE9C2134E652D76DF5BE11A51063D18FE63AC38F06CA613A6BE6FFF9399A491C275627360E723152C702974F7E1E3AF2BC0763F
Malicious:	false
Preview:	A..T.[.OW.w...m....v..(.!.,.Gc..r...E.t....+V.`....~.w.e...A.....+XW...Xow.>(.!u.RX.........p...[.|.y..T...>...R.4O|.q.;.\U..\.?k.h..1!.....&=....c.:sFG..~..MZ.{E5...&..L....e...Y..IY.e..m.Q <.X..... p5M].7e.P...y..da.YRX6..@.*.:...M[..&.O..3.n..~C.....oW*K..sW.-.....=.]...Q_../%`...'..-.;q..yR=....mh.p.}=....7R.. `...2..c.~.N....D..PI....Q..].D...../.....IT`.....^)....;aIF...^.N.....@..g.<ag.L....Q.$u bd....`.,.`6....-_.....S.Q.....&W..*ZS7[.n.P..>|.y...n..fZ..._c.]...&....5..k#2$.'.....8.n.....T7}.zHcf..@Y..4.5..7rt-.1...LnL.h.....pe...c[.z... dQ..r...._...P?.....9...pH7H..5.UO..X9.J.).RK.M.4..R....k..Ak.t.j...}.&.{#6..1+K a.d*...".O3...+:.^...?.....@,mB.b....q..4l...at.... ... Q:@....,.....Y...o.u.....,'.....l0..c.3.....(.. ..|...@..].=.>.^D....}E.....P1W.Y.....M..b...9.....(.....<.=..1!..z....V.]x.l9....k?..DEEB..B[!I..>.....}R.u..["lQ;-.P..[....\>]%0B~:....z....P...\nI..t.Jr[.....N.R.v

C:\Users\user\Desktop\LSBIHQFDVT\ZQIXMVQGAH.xlsx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.979914364379438
Encrypted:	false
SSDEEP:	192:65doJBeuD/TEEaWMOVPkCmE9Gy4sY/SIMvlgV+n:moHeuD7EEWUPdzwSIMNZ
MD5:	2FB1513EDEFA0C8EF8AE7C8AB410049F
SHA1:	3AFF715E3EDFCBEE3801A6D81088875B2E941C9C
SHA-256:	DDDE7183DA60E6526499CDF42FBEA175FCCC2DC61B64A59DD94E08D0B0DDC8F2
SHA-512:	0E6C46B7457C5472120757FABDE9C2134E652D76DF5BE11A51063D18FE63AC38F06CA613A6BE6FFF9399A491C275627360E723152C702974F7E1E3AF2BC0763F
Malicious:	false
Preview:	A..T.[.OW.w...m....v..(.!.,.Gc..r...E.t....+V.`....~.w.e...A.....+XW...Xow.>(.!u.RX.........p...[.|.y..T...>...R.4O|.q.;.\U..\.?k.h..1!.....&=....c.:sFG..~..MZ.{E5...&..L....e...Y..IY.e..m.Q <.X..... p5M].7e.P...y..da.YRX6..@.*.:...M[..&.O..3.n..~C.....oW*K..sW.-.....=.]...Q_../%`...'..-.;q..yR=....mh.p.}=....7R.. `...2..c.~.N....D..PI....Q..].D...../.....IT`.....^)....;aIF...^.N.....@..g.<ag.L....Q.$u bd....`.,.`6....-_.....S.Q.....&W..*ZS7[.n.P..>|.y...n..fZ..._c.]...&....5..k#2$.'.....8.n.....T7}.zHcf..@Y..4.5..7rt-.1...LnL.h.....pe...c[.z... dQ..r...._...P?.....9...pH7H..5.UO..X9.J.).RK.M.4..R....k..Ak.t.j...}.&.{#6..1+K a.d*...".O3...+:.^...?.....@,mB.b....q..4l...at.... ... Q:@....,.....Y...o.u.....,'.....l0..c.3.....(.. ..|...@..].=.>.^D....}E.....P1W.Y.....M..b...9.....(.....<.=..1!..z....V.]x.l9....k?..DEEB..B[!I..>.....}R.u..["lQ;-.P..[....\>]%0B~:....z....P...\nI..t.Jr[.....N.R.v

C:\Users\user\Desktop\LSBIHQFDVT\uCLrcwQ_readme_.txt	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	3762
Entropy (8bit):	5.731391626840331
Encrypted:	false
SSDEEP:	48:L9k0ZzV7L/vNbXGZULVDgUp4qNiiE6bm1c0rfWejhAe/YAliM3PXnLHrYxgkH69H:L95zhLNbXGZUe7Ka6pU6i9fLrvE69UST
MD5:	C75AC33345088DA90A7527CE91E7D9B6
SHA1:	89F6095CA18A0C9BB57C79E727B66DF2A36459D3
SHA-256:	89ACED8641EBD571391EBECFF4C6665B49068038712135392F066BF095D99042
SHA-512:	5C159E68B9AB5EFBFA09E57AD65A3081C0A2EB5A1056767681EEB30391AF7524F7F24C2706858B74465086E411D91AF498C266FCF265D87ADF6C4C7BC77A3CE
Malicious:	false
Preview:	-------=== Your network has been infected! ===-------.....********** DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED ********** .....All your documents, photos, databases and other important files have been encrypted and have the extension: .bCcBDeabea.....You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!.....The only way to restore your files is to buy our special software. Only we can give you this software and only we can restore your files!.....We have also downloaded a lot of private data from your network....If you do not contact as in a 3 days we will post information about your breach on our public news website (avaddongun7rngel.onion) and after 7 days the whole downloaded info.....You can get more information on our page, which is located in a Tor hidden network.....How to get to our page...----------

C:\Users\user\Desktop\PALRGUCVEH.png	
Process:	C:\Users\user\Desktop\ab.exe

C:\Users\user\Desktop\PALRGUCVEH.png	
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976748120492981
Encrypted:	false
SSDEEP:	192:3rrR909YAleD4ivG8ZmhnazUi+Sj8GTaV+n:pmeAvcGkDoNSjj
MD5:	BA1115F85960C4D0C9DE6123AFF2CF8D
SHA1:	B37463FCAEB0219662C02E6C8939AC3922511321
SHA-256:	6FFADFAA4EBE727073EA18AC9CA1FC5E915D7C4A433D9B7E89F608741967F0EE
SHA-512:	A6FF88435D43913C9E5280232490E1D6AE2167BDBF740ED4E2A28015EBEFC5B10AE5E31EF6EF153276A209C3FE8667562988D01FAE560949AE3C3EF1BBF035F(
Malicious:	false
Preview:	C.....E...&..... .9.17.....P..J.Hfd...n...,.kB...5.Q..%a.R.....[..r...Du.....uh7$T...[..M..j....z....?. .r.....-.".aks...N...R....Q.@.d.....G..ZUQ.\|.=.0P.r.0v...wKi...K..4....."....y<~ a.d..w.k...m.+{d.....:f..0..D.7.....v..._l.e.>...c.$?.W.v8.j...."..r..0.Uu.gY`]6.3.;..gl...X@6.....W..D3..f...6.....O...38.....5..&.\.2k*....?.....x.;..S...?t.7!V...eY...._.8.C..se~.o....y .u.cQ.\c.u..sc...r...h.....{...R.`..+..G.3..%3E.;>#....`.B..TV.YEj~.:....Vf.....?..|6.T.X.d..a.dK.<. ...5....Y%[..C5H".....N..d-.J.....gU.(..W.."S.u.....en.P.....Q..@}....TpS..jm8 ..v..D@S.<b.r..1Y..r=...9...'..1B$.]...H.h...8.`..].L...f.c.PZC.....#.....Y....L..*#.....E.}.~...e.{.(..G.....F...-.L.6/~...z...~..c...zeD..hD.kW.q.4.....~..!.1[UES..../K.7.n...?Hp.a.z$.L ..9.....1.z.....!C.....,.+.N0.^..J!/NB..040...^.h..0.).....c...a.:...SVS.'..3.}A.Et.....4...N...\m.+....1.m..P.o...95...\L..n4....*..uK.].k.]...,.....X9.....ia.....a..

C:\Users\user\Desktop\PALRGUCVEH.png.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976748120492981
Encrypted:	false
SSDEEP:	192:3rrR909YAleD4ivG8ZmhnazUi+Sj8GTaV+n:pmeAvcGkDoNSjj
MD5:	BA1115F85960C4D0C9DE6123AFF2CF8D
SHA1:	B37463FCAEB0219662C02E6C8939AC3922511321
SHA-256:	6FFADFAA4EBE727073EA18AC9CA1FC5E915D7C4A433D9B7E89F608741967F0EE
SHA-512:	A6FF88435D43913C9E5280232490E1D6AE2167BDBF740ED4E2A28015EBEFC5B10AE5E31EF6EF153276A209C3FE8667562988D01FAE560949AE3C3EF1BBF035F(
Malicious:	false
Preview:	C.....E...&..... .9.17.....P..J.Hfd...n...,.kB...5.Q..%a.R.....[..r...Du.....uh7$T...[..M..j....z....?. .r.....-.".aks...N...R....Q.@.d.....G..ZUQ.\|.=.0P.r.0v...wKi...K..4....."....y<~ a.d..w.k...m.+{d.....:f..0..D.7.....v..._l.e.>...c.$?.W.v8.j...."..r..0.Uu.gY`]6.3.;..gl...X@6.....W..D3..f...6.....O...38.....5..&.\.2k*....?.....x.;..S...?t.7!V...eY...._.8.C..se~.o....y .u.cQ.\c.u..sc...r...h.....{...R.`..+..G.3..%3E.;>#....`.B..TV.YEj~.:....Vf.....?..|6.T.X.d..a.dK.<. ...5....Y%[..C5H".....N..d-.J.....gU.(..W.."S.u.....en.P.....Q..@}....TpS..jm8 ..v..D@S.<b.r..1Y..r=...9...'..1B$.]...H.h...8.`..].L...f.c.PZC.....#.....Y....L..*#.....E.}.~...e.{.(..G.....F...-.L.6/~...z...~..c...zeD..hD.kW.q.4.....~..!.1[UES..../K.7.n...?Hp.a.z$.L ..9.....1.z.....!C.....,.+.N0.^..J!/NB..040...^.h..0.).....c...a.:...SVS.'..3.}A.Et.....4...N...\m.+....1.m..P.o...95...\L..n4....*..uK.].k.]...,.....X9.....ia.....a..

C:\Users\user\Desktop\PWCCAWLGRE.mp3	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9812873138034055
Encrypted:	false
SSDEEP:	192:lOCDIKuuUlelrOXUXLwnytaaYfrNcH2IqrkWuGD+jSnN4RsLy4V+n:l8xelCXUL9taqhWkpGHnN4mS
MD5:	3DCD8E5F45170DEA1EC9F33642B9D569
SHA1:	B05184D94DFFFB07C370F7C468349F4D4FDCF449
SHA-256:	D8ED18B2FFDE804F4BAB77442C7EAB32B6BECA2AA6FA3A0D850DDDD29EF5AD9B
SHA-512:	3069519753509F700C1ADE63F6AECA6FDD26CFD9C2BB0B80D178151F54498BDB42B440E51DC1BAD58B8C43E296D04AF2E543713538B0E5A4D5B6EE2F228B72I 9
Malicious:	false
Preview:	3....w.{..t...<z.FAs)R%.....[5.X....a...[....xE....*.e..>((o+.."b.....I(.?Z.5ZV....*...c.....q..mJ .c.....-.....A.lMy.....\.A+{..Q.W;..PA[..#G....D.w.{..g.D.Jd(...s'..^p...n..TRA.`..iE.HkH ..!.\.....V.c.....\..$..!Vxa..e._..f.E....NO.bt...W.k9....Ic.s.`...X...9)ZB.....r.....]...../.....F.:..2.....G.`...i|.....O.u.p.<..:m.|< TE.-....."..,.n.+....c.A.j.s.,o..Y.8.(.}..JfN.+>#4.....Z W....Fo.X."o..P..n...jD....I.B.e.....A.....Z.OZ.S.f.l.hL..?....f.;..... .....')..)..../.w.....7.[.iMvH..\.U.7%...U...BN.{.....w...23,k/....D<.....>...`..I.Og41...:.vd....v@....M...,..HLg4"Tcu.(..^..T ..Is.&<f[..X.mW..8!..}r...../..A.4k.[...,...9r.....e.....I.1.1.....g...h.....lN..n.,..rVO'..`.N}m...=c...a....w..."..U.a....5.O.Uh*...jm^.#{0A....|&.^.....Uu...`...PM....AB.....w..6".. [...K...3....[&n..F.F.h.Ggo.wv.....d...P9R...`....?}...`.}.....L...T.?G.....He.E.....`.....Q...W....._.....f..n;zY.Y.....-(0.F.....r..BME{.3...I..y..2

C:\Users\user\Desktop\PWCCAWLGRE.mp3.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9812873138034055
Encrypted:	false
SSDEEP:	192:lOCDIKuuUlelrOXUXLwnytaaYfrNcH2IqrkWuGD+jSnN4RsLy4V+n:l8xelCXUL9taqhWkpGHnN4mS
MD5:	3DCD8E5F45170DEA1EC9F33642B9D569
SHA1:	B05184D94DFFFB07C370F7C468349F4D4FDCF449

C:\Users\user\Desktop\PWCCAWLGRE.mp3.bCcBDeabea (copy)	
SHA-256:	D8ED18B2FFDE804F4BAB77442C7EAB32B6BECA2AA6FA3A0D850DDDD29EF5AD9B
SHA-512:	3069519753509F700C1ADE63F6AECA6FDD26CFD9C2BB0B80D178151F54498BDB42B440E51DC1BAD58B8C43E296D04AF2E543713538B0E5A4D5B6EE2F228B72I 9
Malicious:	false
Preview:	3....w.{..t...<z.FAs)R%.....[5.X....a...[....xE....*.e..>((o+..''b.....I(.?Z.5ZV....*...c.....q..mJ .c.....-.....A.lMy.....\.A+{..Q.W;..PA[..#G....D.w.{..g.D.Jd(...s'..^p...n..TRA.`..iE.HkH ..!.\....V.c.....\..$..!Vxa..e._..f.E....NO.bt...W.k9....Ic.s.`...X...9)ZB.....r.....].....//.....F.:..2.....G.`...i|.....O.u.p.<..:m.|< TE.-.....''..,.n.+....c.A.j.s.,o..Y.8(.}..JfN.+>#4.....Z W....Fo.X."o..P..n...jD....I.B.e.....A.....Z.OZ.S.f.l.hL..?....f.;..... .....')..)..../.w.....7.[.iMvH..\.U.7%...U...BN.{.....w...23,k/....D<.....>...`..I.Og41...:.vd....v@....M..,..HLg4"Tcu.(..^..T ..Is.&<f[..X.mW..8!..}r...../..A.4k.[...,...9r.....e.....I.1.1.....g...h.....lN..n.,..rVO'..`.N}m...=c...a....w...''..U.a....5.O.Uh*...jm^.#{0A....|&.^.....Uu...'`...PM....AB.....w..6''.. [...K...3....[&n..F.F.h.Ggo.wv.....d...P9R...`....?}...`.}.....L...T.?G.....He.E.....`.....Q...W....._.....f..n;zY.Y.....-(0.F.....r..BME{.3...I..y..2

C:\Users\user\Desktop\QCFWYSKMHA.png	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.979221173148451
Encrypted:	false
SSDEEP:	192:FU3U/EwS5ET5WIouqh0FM3XcfJuFmD6+VskKO7eI23k5dAV+n:FU36EwS5mIIo1i+XcfJuj+VVWI2U5
MD5:	AC56A88E6FFF6A4D1AF96CEBA58EF941
SHA1:	82C1D65E7DA21727ACE9626C35F73C5B6A36A306
SHA-256:	F4599CC6F6A84D56A6E25B0027A732B051A1FEA4080A4133EC91194EFF978079
SHA-512:	72453A2FAFAF87B9BB59AB83F28813E120977EE765C66163AB23A77862565BEEECCECD76FEBAEF8ED6F7E5C60251ED41BFF344BBE3503C9A782A69211AD383 29
Malicious:	false
Preview:	m....~2..:P.A..E_c..#....*.}.M....y..9...1..3..\..B.....).fL......S.......].Rgg.rA._V..n.u.....h.T@.R..\0....`R ..xS3^|...B...L0.D).0...>(O8.../....^ES...G..S.YH...} ..t....8.....)>e..f...'=b.sZ.... .9C..s^.z.dpA.1...K.l.+.i..ua.....h.q...l..T.....z..ZA;B.?q...JY.I...K...N.a..N.....;..).Pi.$..V..i`~...l.8.....C.m..=.x...V.`.C.O..rg)9.....x.BwUk..NA...nq....o.D.h.m/....%.cO.B.3..dsQ z.....q...yS.J.D+~. ....)/.M...v@>\.=I5..C.%~/.....o..n.....sr.....4y..%..:..@...X.Gxt.f..y.9..ab}.-_..,.!T..8$...../.(:<.;._...} <.....$....y.q...~`@.Ovt?-...9.q..<.D...''....'..u..~dXB. ..Vm.X2.....A=f84.e....{..E.z...[,.a.I.....@L.>x..Ac...W.5D..TSPT...H.T.BJ.4I....t...<.?.h..i/-.b...8.xC7.A.Z~n....S....).,.:../..G...@%...8..?.....7xrr...n...{.An.=f...r.?0.....GT...}8 ..4.M=gY.....3...N=s|'...%A...>n.&.(X.....b...7..L.....e''..X.t-O>z)..@.f..nv..d...w.9#..y..w.F{.....208.[^.J..{(..:2...,...zl...iR..nL.8..''@o.....%[..9.....PCMO

C:\Users\user\Desktop\QCFWYSKMHA.png.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.979221173148451
Encrypted:	false
SSDEEP:	192:FU3U/EwS5ET5WIouqh0FM3XcfJuFmD6+VskKO7eI23k5dAV+n:FU36EwS5mIIo1i+XcfJuj+VVWI2U5
MD5:	AC56A88E6FFF6A4D1AF96CEBA58EF941
SHA1:	82C1D65E7DA21727ACE9626C35F73C5B6A36A306
SHA-256:	F4599CC6F6A84D56A6E25B0027A732B051A1FEA4080A4133EC91194EFF978079
SHA-512:	72453A2FAFAF87B9BB59AB83F28813E120977EE765C66163AB23A77862565BEEECCECD76FEBAEF8ED6F7E5C60251ED41BFF344BBE3503C9A782A69211AD383 29
Malicious:	false
Preview:	m....~2..:P.A..E_c..#....*.}.M....y..9...1..3..\..B.....).fL......S.......].Rgg.rA._V..n.u.....h.T@.R..\0....`R ..xS3^|...B...L0.D).0...>(O8.../....^ES...G..S.YH...} ..t....8.....)>e..f...'=b.sZ.... .9C..s^.z.dpA.1...K.l.+.i..ua.....h.q...l..T.....z..ZA;B.?q...JY.I...K...N.a..N.....;..).Pi.$..V..i`~...l.8.....C.m..=.x...V.`.C.O..rg)9.....x.BwUk..NA...nq....o.D.h.m/....%.cO.B.3..dsQ z.....q...yS.J.D+~. ....)/.M...v@>\.=I5..C.%~/.....o..n.....sr.....4y..%..:..@...X.Gxt.f..y.9..ab}.-_..,.!T..8$...../.(:<.;._...} <.....$....y.q...~`@.Ovt?-...9.q..<.D...''....'..u..~dXB. ..Vm.X2.....A=f84.e....{..E.z...[,.a.I.....@L.>x..Ac...W.5D..TSPT...H.T.BJ.4I....t...<.?.h..i/-.b...8.xC7.A.Z~n....S....).,.:../..G...@%...8..?.....7xrr...n...{.An.=f...r.?0.....GT...}8 ..4.M=gY.....3...N=s|'...%A...>n.&.(X.....b...7..L.....e''..X.t-O>z)..@.f..nv..d...w.9#..y..w.F{.....208.[^.J..{(..:2...,...zl...iR..nL.8..''@o.....%[..9.....PCMO

C:\Users\user\Desktop\QCFWYSKMHA.xlsx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977860329092125
Encrypted:	false
SSDEEP:	192:aaWU3X45lr4yiRaqoPpsuRY8VQhf2afN3zuzRu4glqbV+n:GU3sdGRaqoqJ2QhfDN3zAu3J
MD5:	0611F51D2DA25AF887A58B5C9A5A41A3
SHA1:	528361487F7509797D0DC8ACBA7116423CEADB36
SHA-256:	7C9E3B1448A162AF2CC26E550E37840FF21DDCDD4A0D792CADA9E438189E94FB
SHA-512:	1884254663CB20584EA91435F269482D225BFD513BF06EAD239929DFB980E5BC8469F81205AE7495FBCE8622A3539A9F99B021A3DFD9859FA07ED63D84D6826E
Malicious:	false

C:\Users\user\Desktop\QCFWYSKMHA.xlsx	
Preview:	....E..5.h.Tt..n.(.sV9..2.B0..$.a..\C.....W..*.T.g..[.....bK..9.;u..pr.....r`....+.v.X'...:Q{..-.. ..+.]K.yD.r.vM<t.L..\|....y/.&.:.V1..V.P..w{.p..*....0..Py.%.....@:dG.lys.m'7.../../J.W.c.* [.,...u.-m...++.].,.<.s..t...O.)..Z.....->C.....Qu.j.)N.x.....`..!....BK.WCB8..0..qR.1=.^s.B.r.ZZ.[&....jU~.....U....A.%..S..Td].yf.{....{..s..NmN.....e3.rb...g+.&G.&.$.....e..d.*. ..._.cO.+.07.....c.d..@Z..J...U..+R-.....i.....7.;.D..[.Nt..~bG^f...p.+.$....)*O.....0.F.RP>+.....?.9....6=L2...5.f..3...W.H.J...>&.,.....s.....Y&..).u.....+...}...$.....iz"... ...uk.....".K ..K.T.....2....q.j..G.b..q...$.:A...LB.....;.zt...st..\ .q4...8;...f....66.Q4..D.Cp.^...?.9B.9A.1.....5..J.f..K.....;.c.BX.A5...o .C....0. .o.u+..r.D.l.Dg.k.....mE...h8...b~L..4Y.{...<2c7.)b.. .6.....pfU'B..#.l.Q....]... ..B.C..d.dv&f*.L.;.}.U.....`._.R3~..{M._...<I..U.....J".<.....?*P..r..F.G..7..vcQ".r.....'^..v.....ywtPL.I..F..".....L.]zc.....`?wgu..s
C:\Users\user\Desktop\QCFWYSKMHA.xlsx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977860329092125
Encrypted:	false
SSDEEP:	192:aaWU3X45lr4yiRaqoPpsuRY8VQhf2afN3zuzRu4glqbV+n:GU3sdGRaqoqJ2QhfDN3zAu3J
MD5:	0611F51D2DA25AF887A58B5C9A5A41A3
SHA1:	528361487F7509797D0DC8ACBA7116423CEADB36
SHA-256:	7C9E3B1448A162AF2CC26E550E37840FF21DDCDD4A0D792CADA9E438189E94FB
SHA-512:	1884254663CB20584EA91435F269482D225BFD513BF06EAD239929DFB980E5BC8469F81205AE7495FBCE8622A3539A9F99B021A3DFD9859FA07ED63D84D6826E
Malicious:	false
Preview:	....E..5.h.Tt..n.(.sV9..2.B0..$.a..\C.....W..*.T.g..[.....bK..9.;u..pr.....r`....+.v.X'...:Q{..-.. ..+.]K.yD.r.vM<t.L..\|....y/.&.:.V1..V.P..w{.p..*....0..Py.%.....@:dG.lys.m'7.../../J.W.c.* [.,...u.-m...++.].,.<.s..t...O.)..Z.....->C.....Qu.j.)N.x.....`..!....BK.WCB8..0..qR.1=.^s.B.r.ZZ.[&....jU~.....U....A.%..S..Td].yf.{....{..s..NmN.....e3.rb...g+.&G.&.$.....e..d.*. ..._.cO.+.07.....c.d..@Z..J...U..+R-.....i.....7.;.D..[.Nt..~bG^f...p.+.$....)*O.....0.F.RP>+.....?.9....6=L2...5.f..3...W.H.J...>&.,.....s.....Y&..).u.....+...}...$.....iz"... ...uk.....".K ..K.T.....2....q.j..G.b..q...$.:A...LB.....;.zt...st..\ .q4...8;...f....66.Q4..D.Cp.^...?.9B.9A.1.....5..J.f..K.....;.c.BX.A5...o .C....0. .o.u+..r.D.l.Dg.k.....mE...h8...b~L..4Y.{...<2c7.)b.. .6.....pfU'B..#.l.Q....]... ..B.C..d.dv&f*.L.;.}.U.....`._.R3~..{M._...<I..U.....J".<.....?*P..r..F.G..7..vcQ".r.....'^..v.....ywtPL.I..F..".....L.]zc.....`?wgu..s

C:\Users\user\Desktop\QNCYCDFIJJ.docx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978547796797249
Encrypted:	false
SSDEEP:	192:4mgdiDazuDUBBF8oj47J2PLk4moGHsWb0MV+n:4rymuDqBB47AjkuiU
MD5:	1AF33DC577EC48E7265C09F31EDA0AAA
SHA1:	E1C19E4F2FD86772160856AFFB9E27E885E9395D
SHA-256:	3B40A5C77E644B5CC5A4149547E12F756A6248D13D3C9225D49E042D23DF94AC
SHA-512:	2CA3B078808E86356ECB66C35AAEC4BCFA0559A85F1D5B4C540EE8B41F59B1F6B80E2AB14059E8A56FDF1B5548EADF59F3B4A7EDAA85031C2066BD34C35A52 31
Malicious:	false
Preview:	..?.....<..~..6..e...w0.....h?..L}.QAc;.....V.[...?...R..j1.....,...R.gL..hR:.K.S.mv..YtR..L.)...3.zN=<K.....m.k.]c/..3.....+.....$.IlgF.J..6&P.r..nq{..^{`)..dl.q.7.....m.D. V<....aE..j. @..FN.....2d.`:.d.5&i.(I}...7m..o....@..m....P.=x.s.....o.{6....5...N.E&..b.j...JQQ&..4L_..5...a..r.&w..L$r...).....!.gb(....0.....+ .8....qP..q>p..Nwz.(b.A$X.6.....\L....u...Fd..(...{. '.y.h4..:6..N._.....?.s`J.(._.....c.[...C.'t8>..-qh.z/....I....#.I.Du...:O.E....hR..G"lg.}.q..k..[Z.'..k..l..#.:HzP.C.8..%qf>..B..%.Fk..|.G.Vvh.3...5.xW.1Oh..h..`....X.&WJ..R..._.j..Y.. ....XN.w...W@.O%./....E.Fs..i.t.(....{."......K......S..i.....PMq..f.CYV.z....`.[S..'4.u,H..a.;...g..0p=..$.YR...j..1...AY#J..ODZ|...O.6yM.V3..(i.`?.....(.@....n.7..+.?.s5....z.....E6.:..$.- ..8Ei.5Y.raL..y.s..]x.e...2.vA....q.3.|..g..].f.....3....=.....F.....v"L.T.1...d...6|.";..*.$../b.....h..-G..dO@.....n..f?...8W..G...._7...u.....xz...T..
C:\Users\user\Desktop\QNCYCDFIJJ.docx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978547796797249
Encrypted:	false
SSDEEP:	192:4mgdiDazuDUBBF8oj47J2PLk4moGHsWb0MV+n:4rymuDqBB47AjkuiU
MD5:	1AF33DC577EC48E7265C09F31EDA0AAA
SHA1:	E1C19E4F2FD86772160856AFFB9E27E885E9395D
SHA-256:	3B40A5C77E644B5CC5A4149547E12F756A6248D13D3C9225D49E042D23DF94AC
SHA-512:	2CA3B078808E86356ECB66C35AAEC4BCFA0559A85F1D5B4C540EE8B41F59B1F6B80E2AB14059E8A56FDF1B5548EADF59F3B4A7EDAA85031C2066BD34C35A52 31
Malicious:	false
Preview:	..?.....<..~..6..e...w0.....h?..L}.QAc;.....V.[...?...R..j1.....,...R.gL..hR:.K.S.mv..YtR..L.)...3.zN=<K.....m.k.]c/..3.....+.....$.IlgF.J..6&P.r..nq{..^{`)..dl.q.7.....m.D. V<....aE..j. @..FN.....2d.`:.d.5&i.(I}...7m..o....@..m....P.=x.s.....o.{6....5...N.E&..b.j...JQQ&..4L_..5...a..r.&w..L$r...).....!.gb(....0.....+ .8....qP..q>p..Nwz.(b.A$X.6.....\L....u...Fd..(...{. '.y.h4..:6..N._.....?.s`J.(._.....c.[...C.'t8>..-qh.z/....I....#.I.Du...:O.E....hR..G"lg.}.q..k..[Z.'..k..l..#.:HzP.C.8..%qf>..B..%.Fk..|.G.Vvh.3...5.xW.1Oh..h..`....X.&WJ..R..._.j..Y.. ....XN.w...W@.O%./....E.Fs..i.t.(....{."......K......S..i.....PMq..f.CYV.z....`.[S..'4.u,H..a.;...g..0p=..$.YR...j..1...AY#J..ODZ|...O.6yM.V3..(i.`?.....(.@....n.7..+.?.s5....z.....E6.:..$.- ..8Ei.5Y.raL..y.s..]x.e...2.vA....q.3.|..g..].f.....3....=.....F.....v"L.T.1...d...6|.";..*.$../b.....h..-G..dO@.....n..f?...8W..G...._7...u.....xz...T..

C:\Users\user\Desktop\QNCYCDFIJJ.jpg	
Process:	C:\Users\user\Desktop\ab.exe

C:\Users\user\Desktop\QNCYCDFIJJ.jpg	
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.980538899760363
Encrypted:	false
SSDEEP:	192:ZAE4/1zdV9XFMaEhv3ZorCLLH6Qvu9I6X2Zn+a9PyG/wuF2csvV+n:Zop4am/ZorC/HRvu9IWSnFyG/wun
MD5:	9CC5974F5685D94A4F42A3BCD8D17FCE
SHA1:	177F93B0C98EE538D2088DEC3ABA28F180545B5E
SHA-256:	3A2E4553302AD38E338B6E291F2ADD041E1AC5C59248AEFA1F2BEEDB44D444C5
SHA-512:	FDF7A1F89C847CB4AE155568ECC66D9515C7F7727C9F3E960DF7B45EFBD4F4F40D0AE4156DEC3B7F7C14FF9D558D460BE8CDB5E256A607AAA6B217362F0440AF
Malicious:	false
Preview:	Z.....i..JW.NrPQ..5.l:.&w;....k.,...SaY7..}#..9C^.ar.*..Y."...J.9t...k.1....aN..%|V>.....K.....(.....,....T...N}..1...n1.f......b.R......A.F;.aUUB..g.O4...4.7.Y. ..c...:.....,..>~.9.`9k13.. Y..&.ZD....C.c4..l..-.5.5..OX.I.'1y3%7..s..S.....km...h.3.....J.]9{o^<+0=.Qf./U..(.n....Y.....z.O..@.JI.u....D..{:...4o..B.:S..(n..0..5.z...G...M3H%.....b....$.bK.+m.b{*d....f.:w`. ..1.....u...4..:Z..9c`.x. .+.O.O.....u.H?....16...K.@F..1.D.....d.F.p2.o2.3..u...=:V.....W...z...'6..\.i.oK.....<".dj...tB.....Q...n....2-z..-M]..2.#.q8...[M...^..#....2.C.....h.9.@`.<H u..*j.4b.G*...4..9.]O4X..B~Ph.a0..HH..j...z#@.n..-:.L..... ..WR.S.qt!M..[.B..E].}..W0..Z..:.b0/GG.....0..o..}....1...p)X..C.;...v...Zu...D,s...f..1..J.R..'..Ei.'=.....*....e..P.2..-.4..B6. <.....;.....w. q..c.\|.4..(IP.W.RQ.?...d...;.w..W...:..`..}...Ux..X.=.dy.L.c.d...O...s.[~..T...y/..J...;.XP).....'....!%....t..Y...U....)m.z.s2...x..$..u.....;V)<.:...A...

C:\Users\user\Desktop\QNCYCDFIJJ.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.980538899760363
Encrypted:	false
SSDEEP:	192:ZAE4/1zdV9XFMaEhv3ZorCLLH6Qvu9I6X2Zn+a9PyG/wuF2csvV+n:Zop4am/ZorC/HRvu9IWSnFyG/wun
MD5:	9CC5974F5685D94A4F42A3BCD8D17FCE
SHA1:	177F93B0C98EE538D2088DEC3ABA28F180545B5E
SHA-256:	3A2E4553302AD38E338B6E291F2ADD041E1AC5C59248AEFA1F2BEEDB44D444C5
SHA-512:	FDF7A1F89C847CB4AE155568ECC66D9515C7F7727C9F3E960DF7B45EFBD4F4F40D0AE4156DEC3B7F7C14FF9D558D460BE8CDB5E256A607AAA6B217362F0440AF
Malicious:	false
Preview:	Z.....i..JW.NrPQ..5.l:.&w;....k.,...SaY7..}#..9C^.ar.*..Y."...J.9t...k.1....aN..%|V>.....K.....(.....,....T...N}..1...n1.f......b.R......A.F;.aUUB..g.O4...4.7.Y. ..c...:.....,..>~.9.`9k13.. Y..&.ZD....C.c4..l..-.5.5..OX.I.'1y3%7..s..S.....km...h.3.....J.]9{o^<+0=.Qf./U..(.n....Y.....z.O..@.JI.u....D..{:...4o..B.:S..(n..0..5.z...G...M3H%.....b....$.bK.+m.b{*d....f.:w`. ..1.....u...4..:Z..9c`.x. .+.O.O.....u.H?....16...K.@F..1.D.....d.F.p2.o2.3..u...=:V.....W...z...'6..\.i.oK.....<".dj...tB.....Q...n....2-z..-M]..2.#.q8...[M...^..#....2.C.....h.9.@`.<H u..*j.4b.G*...4..9.]O4X..B~Ph.a0..HH..j...z#@.n..-:.L..... ..WR.S.qt!M..[.B..E].}..W0..Z..:.b0/GG.....0..o..}....1...p)X..C.;...v...Zu...D,s...f..1..J.R..'..Ei.'=.....*....e..P.2..-.4..B6. <.....;.....w. q..c.\|.4..(IP.W.RQ.?...d...;.w..W...:..`..}...Ux..X.=.dy.L.c.d...O...s.[~..T...y/..J...;.XP).....'....!%....t..Y...U....)m.z.s2...x..$..u.....;V)<.:...A...

C:\Users\user\Desktop\QNCYCDFIJJ\EFOYFBOLXA.jpg	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.975620479137032
Encrypted:	false
SSDEEP:	192:Nms5Q6dygYLULRtiMBW948Jz8fW1tUuBEQgxZUbV6AeWyQV+n:x5Q6sXLUL41Jwfqt94JWyp
MD5:	56FDCA0F8994852C676076FB15F105F0
SHA1:	5478462C34AE79FED8C1BC5B0AE1D4198C724FC6
SHA-256:	25F32C69D3D6CED7CEE19B942DBBE89DB2D541DAA799ACF6B551A7C835B3B8FF
SHA-512:	3388E84C382B62B1DA4EDB2593A52184A0616F6F2F90BB7078142A94E5BF2788F47C98C62D050B86FA705482F30F7381A43E00239E61E0833957ADDABF948F9E
Malicious:	**true**
Preview:	.CE..A.'..1.....L.1.]N.$.gu..n.{.:.7...!..0(..i..#.e...kO.5....5e..,v~...{...,Qbd/.....h.A....j...J,...L+...oK!.K..b.5.a.S.....V....6:J.y...).#.p....0....Ji.r.(..?1\|.J.q2en.....j.@*....\|..?-.5 .. #...R..4.7.^."..!....._.=J.mH..`....gM.E...T..xSSy.;/(.i....a..T.y.y..\6...#.s<h....9..m2..}..v(.ztM..<....1.Q.1..Q....R1...g-.?..gPm...mf.k...V9.b.P.\|.....u}9...W...x..r..M.%...*A..j.Q.....e j..&.).5.._.l........P..=.;.....K.a..a.....Lk.\|.....+...8.:=v8.I.O....N...).q).....)&2..eH....C.....Y=..vB&...DhY..G:.&?4..L\|.KAC..E..''(..K.0.....c(..;C!.q.$ZM.....f.@b..)#PN.l.a.B3....0.t.... .q.x.+xbl$e:,6.1..2.S..._..6:.i.w....Y2S..cnG..R.a.....R....rv..u.IbC5..\|.)..uJi.l.k...Pf.....>1..R.{#..W...!*..[2'.....\.$.& /.....T).y..".H.....'..{. ....;.....)..S.I..%A...p...&.\...+...xa..... V.?....A..Sq.B...D...L.....<^.1.}.v@qn.....C/WU.;.Crl..q.....A.g1{q...x.....6....+.}c(..*.N::....~...p.#@....c...$...Q..2..{O.~^.O.R.3..x).>!IArf

C:\Users\user\Desktop\QNCYCDFIJJ\EFOYFBOLXA.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.975620479137032
Encrypted:	false
SSDEEP:	192:Nms5Q6dygYLULRtiMBW948Jz8fW1tUuBEQgxZUbV6AeWyQV+n:x5Q6sXLUL41Jwfqt94JWyp
MD5:	56FDCA0F8994852C676076FB15F105F0

C:\Users\user\Desktop\QNCYCDFIJJ\EFOYFBOLXA.jpg.bCcBDeabea (copy)	
SHA1:	5478462C34AE79FED8C1BC5B0AE1D4198C724FC6
SHA-256:	25F32C69D3D6CED7CEE19B942DBBE89DB2D541DAA799ACF6B551A7C835B3B8FF
SHA-512:	3388E84C382B62B1DA4EDB2593A52184A0616F6F2F90BB7078142A94E5BF2788F47C98C62D050B86FA705482F30F7381A43E00239E61E0833957ADDABF948F9E
Malicious:	false
Preview:	.CE..A.'..1.....L.1.]N.$.gu..n.{.:.7...!..0(..i..#.e...kO.5....5e..,v~...{...,Qbd/........h.A....j...J,...L+...oK!.K..b.5.a.S.....V....6:J.y...).#.p....0....Ji.r.(..?1|.J.q2en....j.@*....\|..?-.5 .. #...R..4.7.^."..!....._.=J.mH..`....gM.E...T..xSSy.;/(.i....a..T.y.y..\6...#.s<h....9..m2..}..v(.ztM..<....1.Q.1..Q....R1...g-.?..gPm...mf.k...V9.b.P.\|.....u}9...W...x..r..M.%...*A..j.Q.....e j..&.).5.._.l........P..=.;.....K.a..a.....Lk.\|.....+...8.:=v8.I.O....N...).q).....)&2..eH....C.....Y=..vB&...DhY..G:.&?4..L\|.KAC..E..''(..K.0.....c(..;C!.q.$ZM.....f.@b..)#PN.I.a.B3....0.t.... .q.x.+xbI$e:,6.1..2.S..._..6:.i.w....Y2S..cnG..R.a.....R....rv..u.IbC5..].)..uJi.I.k...Pf.....>1..R.{#..W...!*..[2'.....\.$.& /.....T).y..''.H.....'..{. ....;.....)..S.I..%A...p...&.\...+...xa..... V.?....A..Sq.B...D...L.....<^.1.}.v@qn.....C/WU.;.Crl..q.....A.g1{q...x.....6....+.}c(..*.N:....~...p.#@....c...$...Q..2..{O.~^.O.R.3..x).>!IArf

C:\Users\user\Desktop\QNCYCDFIJJ\PALRGUCVEH.png	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978353269558998
Encrypted:	false
SSDEEP:	192:llJYaHSWMiN6PrTjsOoEUNHu+UvuYTJFRZy+2arOV+n:CJYaHlMiIrsOohg+A1Zyw
MD5:	0DB5E91DC7F4D76BF8600F70451C2521
SHA1:	98C5EF5BA7E819D39D1736FFE97BAD948CFEBEA6
SHA-256:	3B275F33A89D9000E2CC28691DD344A03CA92577B488E2CA41D622A0058B4DDE
SHA-512:	AB55398EC9CC5D7A8BEAE202109229CE2AA37873C709B9D393B4CF9565033D28268C6237FD0421DF13FD734027BD71ABBB058BD7F03D1AAF0BD6971DF9C00E3
Malicious:	false
Preview:	.....DJ.f.E.Z<.T...p....!....z....U3...Jql.b ...66..7P.=.....b.y=.2..R:u#.)...r....j..B.....fZ..N.....}z...{..W...t.8\7.s.....z.#d...6.a.q....n...C..-...M .....~..R.$.....hl....\|.%...2.. M..W3.v..r.....=...n....".y&kD.b.w...v...nB.....Z'.KL..f..scw...x.F..[.....A.....X..47R`.L..1.. .-...!A.Vu.Q.mJt.UN....,.. ...7...g..).....>J.l.l...x."....U.*.-:DL.>.I..^/.9...z'hL1..n...~\...C\ (m.}.%Q...!.....s;U...I....*.....$..,...L.C.I.V.g\..h{..ug.7R.';..k}.=...#_.j.$w.aL.!...F?..@.r..V0....D._.Z..i....=..-.R.L./ T.....W...k..i.E.....A..2...|...g..hs..V..k.'....j.p5'..2.9....s.U..... <....k9..O...X;...B3...{k...zz.I.H....aDP.....z.(y.L-F...`k.l....@.O.3..3.b..y=9t.`...U..p...d]2..@~?.....wK...TT...;v..[o.....I.....vu..5i:c...1...z...vp...7.M...JujD.n)..N|~5.6..U|...~*... .T.zY...\B.rQ1.\D3v.p!..gN.^....%,.RW..]v7t.U.+u.....|8|n.....nT.K.. .}..+I.....Z....L..w.p.h.G.=j.8.b.W....I..%6....i....;.U.~...uU`.

C:\Users\user\Desktop\QNCYCDFIJJ\PALRGUCVEH.png.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978353269558998
Encrypted:	false
SSDEEP:	192:llJYaHSWMiN6PrTjsOoEUNHu+UvuYTJFRZy+2arOV+n:CJYaHlMiIrsOohg+A1Zyw
MD5:	0DB5E91DC7F4D76BF8600F70451C2521
SHA1:	98C5EF5BA7E819D39D1736FFE97BAD948CFEBEA6
SHA-256:	3B275F33A89D9000E2CC28691DD344A03CA92577B488E2CA41D622A0058B4DDE
SHA-512:	AB55398EC9CC5D7A8BEAE202109229CE2AA37873C709B9D393B4CF9565033D28268C6237FD0421DF13FD734027BD71ABBB058BD7F03D1AAF0BD6971DF9C00E3
Malicious:	false
Preview:	.....DJ.f.E.Z<.T...p....!....z....U3...Jql.b ...66..7P.=.....b.y=.2..R:u#.)...r....j..B.....fZ..N.....}z...{..W...t.8\7.s.....z.#d...6.a.q....n...C..-...M .....~..R.$.....hl....\|.%...2.. M..W3.v..r.....=...n....".y&kD.b.w...v...nB.....Z'.KL..f..scw...x.F..[.....A.....X..47R`.L..1.. .-...!A.Vu.Q.mJt.UN....,.. ...7...g..).....>J.l.l...x."....U.*.-:DL.>.I..^/.9...z'hL1..n...~\...C\ (m.}.%Q...!.....s;U...I....*.....$..,...L.C.I.V.g\..h{..ug.7R.';..k}.=...#_.j.$w.aL.!...F?..@.r..V0....D._.Z..i....=..-.R.L./ T.....W...k..i.E.....A..2...|...g..hs..V..k.'....j.p5'..2.9....s.U..... <....k9..O...X;...B3...{k...zz.I.H....aDP.....z.(y.L-F...`k.l....@.O.3..3.b..y=9t.`...U..p...d]2..@~?.....wK...TT...;v..[o.....I.....vu..5i:c...1...z...vp...7.M...JujD.n)..N|~5.6..U|...~*... .T.zY...\B.rQ1.\D3v.p!..gN.^....%,.RW..]v7t.U.+u.....|8|n.....nT.K.. .}..+I.....Z....L..w.p.h.G.=j.8.b.W....I..%6....i....;.U.~...uU`.

C:\Users\user\Desktop\QNCYCDFIJJ\QNCYCDFIJJ.docx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.975121053775242
Encrypted:	false
SSDEEP:	192:RwbPrGt4MpOUPYhwI/iI2Thy8+4+NJBHKB4nk8/3FgILIuv2SV+n:+jU/pOUg2grXJlKBUvFgIbi
MD5:	2D72C7C1572D9967D41331970844F005
SHA1:	864D2B658A51BE707EC40AFEC21C4D0FA452FEA1
SHA-256:	B3F9670BB1451A22903E30E801B2DAC1D247E4C972431BD0648DF2A3D23FB552
SHA-512:	48C0DB4EAEC79BE3E529586E5402FFD470A5CDE85A676E765194DC8FE75B38A9E05E99932AFF12550E1D2C794B82A9AEA5CD7AE178B25B741C3EBF52E8FFB6F0
Malicious:	**true**

C:\Users\user\Desktop\QNCYCDFIJJ\QNCYCDFIJJ.docx	
Preview:	WM....._i...AO.T[.....*\.....5....n\}....;)[...T...eQ...;...)#.....k..%..x...}...r.j...v.`...n.....xH.l.k..V....~...W.|.gn#.t.k.$o.T...BB...X.p T.....\|\_.....ji?.x.M...N=...u7.<....+v.....5.@.E.PQ....-I....]>..t.....X.=.....Lq..4.G....;tN...R.....U..B.....op.8K2.2.g.ua.e.R.:.....j9.^..y.8.)....vu?PL.T.x.x...../.?f6..9.....<.....%..Bp[tLF+....-3.5A...6..~..^R>....7B.u>#..bS...~ml..t .....W0\_..x.2.2.....Q.m..97...%. oj.=...e.c.<T.Nd.....-...gW.A.K..7.w...]Q.pKj..p..?.(.....O...r!.z!b.i.]. .....>..}..lB....f..P3..z.p)Z[<.BR..z....L=....j....9\_F..mh.\_Tp.h....\).....% .f.W!.2.....\|...B....1.~.'...F.pK...Wr....~2Z..[.h~S.....n.....A..{..5i.=..Ti.9..P.Z.F.a.N...-..F>.{.....T.b.zK>.&.Q..6g....Of%,<.~..H....[....$..I.,b.G....t.Y=...d.X..YFF..*~ay.N....g .....K..o^K<...O..v.3.g@...h.r.K.8.n~..LG.X.W....tF.c...).b..#.\...I.[..A.{&5K-sx..v.^.|UT.lL.....4...4W..G..}z....[..$...+....G.{>....7.li...fGC...].?.

C:\Users\user\Desktop\QNCYCDFIJJ\QNCYCDFIJJ.docx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.975121053775242
Encrypted:	false
SSDEEP:	192:RwbPrGt4MpOUPYhwl/il2Thy8+4+NJBHKB4nk8/3FgILIuv2SV+n:+jU/pOUg2grXJlKBUvFgIbi
MD5:	2D72C7C1572D9967D41331970844F005
SHA1:	864D2B658A51BE707EC40AFEC21C4D0FA452FEA1
SHA-256:	B3F9670BB1451A22903E30E801B2DAC1D247E4C972431BD0648DF2A3D23FB552
SHA-512:	48C0DB4EAEC79BE3E529586E5402FFD470A5CDE85A676E765194DC8FE75B38A9E05E99932AFF12550E1D2C794B82A9AEA5CD7AE178B25B741C3EBF52E8FFB6 F0
Malicious:	false
Preview:	WM....._i...AO.T[.....*\.....5....n\}....;)[...T...eQ...;...)#.....k..%..x...}...r.j...v.`...n.....xH.l.k..V....~...W.|.gn#.t.k.$o.T...BB...X.p T.....\|\_.....ji?.x.M...N=...u7.<....+v.....5.@.E.PQ....-I....]>..t.....X.=.....Lq..4.G....;tN...R.....U..B.....op.8K2.2.g.ua.e.R.:.....j9.^..y.8.)....vu?PL.T.x.x...../.?f6..9.....<.....%..Bp[tLF+....-3.5A...6..~..^R>....7B.u>#..bS...~ml..t .....W0\_..x.2.2.....Q.m..97...%. oj.=...e.c.<T.Nd.....-...gW.A.K..7.w...]Q.pKj..p..?.(.....O...r!.z!b.i.]. .....>..}..lB....f..P3..z.p)Z[<.BR..z....L=....j....9\_F..mh.\_Tp.h....\).....% .f.W!.2.....\|...B....1.~.'...F.pK...Wr....~2Z..[.h~S.....n.....A..{..5i.=..Ti.9..P.Z.F.a.N...-..F>.{.....T.b.zK>.&.Q..6g....Of%,<.~..H....[....$..I.,b.G....t.Y=...d.X..YFF..*~ay.N....g .....K..o^K<...O..v.3.g@...h.r.K.8.n~..LG.X.W....tF.c...).b..#.\...I.[..A.{&5K-sx..v.^.|UT.lL.....4...4W..G..}z....[..$...+....G.{>....7.li...fGC...].?.

C:\Users\user\Desktop\QNCYCDFIJJ\SQSJKEBWDT.pdf	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9769649874809625
Encrypted:	false
SSDEEP:	192:2gkXqYhAW7OPb78O8sTh44EIo02Wdj6Ex6NgOyn8NDM1TM0j84V+n:2gkaYn7O8nsl44/o0fCgZ8NDl
MD5:	F90BFD93626100A27EE9CB7895458A58
SHA1:	B1D9ECA7009646151EC1EB46F456BC0CD3B82BF4
SHA-256:	A74214BA0B242C0B0D3BE1ED8FF2342996868CEBEDFB856CF6A41A24981CD901
SHA-512:	A9534F08EE8249B8E3D02BBDB236A38F1BFD38D8767AA83904E54E4EC8239F454865EA9F192AB4AAC0BE8A5689E3BBBE9BDD9D7FDC3DC96E8FB9D39AC4AB9 20D
Malicious:	false
Preview:	X....C....V..38M0..CV.%t2.....g.....#..gs..5Z.....kF.Xg.e.B..:..`l..?.F...u...~..|6.8..q*.>Q*..d...!.c6=F.Ee.YxA...:q.1oM#6.G..[.m..^z..|.E...B.WM...sp. .7....'e&"..r.....yH...w? #S...@..X.e8..RZ...s\.....a7..2.G..xp.2.7N...E..$.~m.v(o0..-...H...J.>(6..d..Pd.,.8.M%..=.U.z...!....J.....@Q....&.0.s.;/.*..1:..T....2..G"M....H..'%&.ftV.G..y..'?R.j.&&8....3. pw..FF.2.x...X.9.....!.V.....c....i.%.D../|[.mX.. .B....z...;7...@.{I.\.b{.EL....F....hlx@..j.....v...S..(K..k.o.(....y2.."....{Y.8.-.,;....D.R...cH...MoL.....E.x.GL1..l.....(+.3.w-j ..2.u\.od;.E...J).Uk.-#>w.5a.....n..Q....g.7....!~..`.c;.O..+.Kq...g.....*xbE|..X.....c@k5.d.:.=W..r.....H..8..)5.....qd..q..sz.j...V..M....pd3}.[I..j.-8KW....z..q3.....aoL.f.:].L.....K.:.n .r.s.m.4s?{P..A \6..Sir.....fo)..c....*.....[..mF....>.>{.d..@...?.7_... ../.....CTG..x:.-.=..._..1i ..<...m./|o^..`6..c..5.it8.M.....p...'Bn.B..a_..D{e&.....k_Uo..I...q..@..

C:\Users\user\Desktop\QNCYCDFIJJ\SQSJKEBWDT.pdf.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9769649874809625
Encrypted:	false
SSDEEP:	192:2gkXqYhAW7OPb78O8sTh44EIo02Wdj6Ex6NgOyn8NDM1TM0j84V+n:2gkaYn7O8nsl44/o0fCgZ8NDl
MD5:	F90BFD93626100A27EE9CB7895458A58
SHA1:	B1D9ECA7009646151EC1EB46F456BC0CD3B82BF4
SHA-256:	A74214BA0B242C0B0D3BE1ED8FF2342996868CEBEDFB856CF6A41A24981CD901
SHA-512:	A9534F08EE8249B8E3D02BBDB236A38F1BFD38D8767AA83904E54E4EC8239F454865EA9F192AB4AAC0BE8A5689E3BBBE9BDD9D7FDC3DC96E8FB9D39AC4AB9 20D
Malicious:	false
Preview:	X....C....V..38M0..CV.%t2.....g.....#..gs..5Z.....kF.Xg.e.B..:..`l..?.F...u...~..|6.8..q*.>Q*..d...!.c6=F.Ee.YxA...:q.1oM#6.G..[.m..^z..|.E...B.WM...sp. .7....'e&"..r.....yH...w? #S...@..X.e8..RZ...s\.....a7..2.G..xp.2.7N...E..$.~m.v(o0..-...H...J.>(6..d..Pd.,.8.M%..=.U.z...!....J.....@Q....&.0.s.;/.*..1:..T....2..G"M....H..'%&.ftV.G..y..'?R.j.&&8....3. pw..FF.2.x...X.9.....!.V.....c....i.%.D../|[.mX.. .B....z...;7...@.{I.\.b{.EL....F....hlx@..j.....v...S..(K..k.o.(....y2.."....{Y.8.-.,;....D.R...cH...MoL.....E.x.GL1..l.....(+.3.w-j ..2.u\.od;.E...J).Uk.-#>w.5a.....n..Q....g.7....!~..`.c;.O..+.Kq...g.....*xbE|..X.....c@k5.d.:.=W..r.....H..8..)5.....qd..q..sz.j...V..M....pd3}.[I..j.-8KW....z..q3.....aoL.f.:].L.....K.:.n .r.s.m.4s?{P..A \6..Sir.....fo)..c....*.....[..mF....>.>{.d..@...?.7_... ../.....CTG..x:.-.=..._..1i ..<...m./|o^..`6..c..5.it8.M.....p...'Bn.B..a_..D{e&.....k_Uo..I...q..@..

C:\Users\user\Desktop\QNCYCDFIJJ\SUAVTZKNFL.xlsx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977333473305457
Encrypted:	false
SSDEEP:	192:3swzRNxhlxBJL1CniRWEkogQInb0ncftkfvNdV+n:3bRNxpBLKEOQIn4cFh
MD5:	96F0F1B578D8866C95A99933FF8CDC02
SHA1:	431317EC5043415D882E62EA531076A9F88F0793
SHA-256:	E7A01672AF61C667647B4F680BC1D9F9D63907DC0F172C5F5B479E923B00946D
SHA-512:	48F76F4C1D20A61A42060EF47DE3BEBE139AA77593820936B48BB3ECB9B634D866C61DE68686CC97C7928250F5042C20B25707EBDF775B2B134CA2EBC229314
Malicious:	false
Preview:	NW..L..N?>i.$.F%....w..^....u*...oU.]y.:.....Xb.rI...[Q)&z.....3...K\|z..L.Xv.o.... =.....V..m.B~.8.*j..G.Q_..1..f=..`...s.Y.r]...Mt..t...B..@L.....\....U?I...}.....9h..?.....*T.U....< .q..:.XXL...c.B...C.....:...Y#{....Vr7.1\|....o.G.]E-.\.DP..i...1W...J...c f%.G..#.D!.....h..t.?i.S.UI..1....y.ksda.<...g....+.e...#.A.A.d.m.m+..B...N.x#...g%.Y.C..a..U...m...l..\|W0..,.nD..)...'.K..rt.....>..U.....H.}."..1.[Bb.{..],:.`D.9....a.YE...`~.....0..5.....Ij....P..+.a@iV.Z.a.R..v\.q.).fo.y....t.3.tK...T5..J.....e.I ..!pe.....N.3..G.Yp..=)....mR]Y..f1m.).U.cr..v..;.>*2I`Ip8e g.....E..<...3.I...m.....K}F8.-\|..9.G.5....+.b.q....`....=..xVZ; .....~o..,k....l...W.X.8`.,. V...d...J.l0e_...*...../...w.+.....y.egx...5...J.\I.N.M..J.}...q..~4.$....1..MJ..H....{.....V@...\,1L .Pu\.d.>...V.....^~..I.r3..:,!*'.|mb....R'.]/>..mF...SG-.....4q..<53G<3{.(.G..^..p.QGe..\.s.E....:j9a..'.....,_.....1d.)..T.d...v.....F.*..*(....l$Sh....)d.....

C:\Users\user\Desktop\QNCYCDFIJJ\SUAVTZKNFL.xlsx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977333473305457
Encrypted:	false
SSDEEP:	192:3swzRNxhlxBJL1CniRWEkogQInb0ncftkfvNdV+n:3bRNxpBLKEOQIn4cFh
MD5:	96F0F1B578D8866C95A99933FF8CDC02
SHA1:	431317EC5043415D882E62EA531076A9F88F0793
SHA-256:	E7A01672AF61C667647B4F680BC1D9F9D63907DC0F172C5F5B479E923B00946D
SHA-512:	48F76F4C1D20A61A42060EF47DE3BEBE139AA77593820936B48BB3ECB9B634D866C61DE68686CC97C7928250F5042C20B25707EBDF775B2B134CA2EBC229314
Malicious:	false
Preview:	NW..L..N?>i.$.F%....w..^....u*...oU.]y.:.....Xb.rI...[Q)&z.....3...K\|z..L.Xv.o.... =.....V..m.B~.8.*j..G.Q_..1..f=..`...s.Y.r]...Mt..t...B..@L.....\....U?I...}.....9h..?.....*T.U....< .q..:.XXL...c.B...C.....:...Y#{....Vr7.1\|....o.G.]E-.\.DP..i...1W...J...c f%.G..#.D!.....h..t.?i.S.UI..1....y.ksda.<...g....+.e...#.A.A.d.m.m+..B...N.x#...g%.Y.C..a..U...m...l..\|W0..,.nD..)...'.K..rt.....>..U.....H.}."..1.[Bb.{..],:.`D.9....a.YE...`~.....0..5.....Ij....P..+.a@iV.Z.a.R..v\.q.).fo.y....t.3.tK...T5..J.....e.I ..!pe.....N.3..G.Yp..=)....mR]Y..f1m.).U.cr..v..;.>*2I`Ip8e g.....E..<...3.I...m.....K}F8.-\|..9.G.5....+.b.q....`....=..xVZ; .....~o..,k....l...W.X.8`.,. V...d...J.l0e_...*...../...w.+.....y.egx...5...J.\I.N.M..J.}...q..~4.$....1..MJ..H....{.....V@...\,1L .Pu\.d.>...V.....^~..I.r3..:,!*'.|mb....R'.]/>..mF...SG-.....4q..<53G<3{.(.G..^..p.QGe..\.s.E....:j9a..'.....,_.....1d.)..T.d...v.....F.*..*(....l$Sh....)d.....

C:\Users\user\Desktop\QNCYCDFIJJ\ZGGKNSUKOP.mp3	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97385858418915
Encrypted:	false
SSDEEP:	192:xjnuFwDrCl9UCeF58cFUlqcmN2W7SNOlXbgweV+n:0wrClselZmN2DK0wL
MD5:	9DCEB64E009429AF62B508BDF1BB8D25
SHA1:	6B81D5024FDB1456DA785193DB339CB21515560B
SHA-256:	3039B3328ABB02A2EEA135565BB7C044665DBF9352A968F716CA46BC3B86DB0A
SHA-512:	CD077EC64325FA6FA1D35404FF2FB798052485E94F99E4A18846200FD2B99D76DB0B5492C510F491E415043614A3315F041D6B88941EEF2BB1BB83400ED53CDE
Malicious:	false
Preview:	y'..`.bX....T.<..)K:N....APO..p...#k.p...}....SJ..&.....7.....;.....d.5.3.q.{....Z]G[....I.^Q..._.I.....8...*.....k/.~.Y.0../....Sd..>=..KH;.6...Fg..^r.N./GMDm ...Y1...,|A`...X..<. H..Cm....X....i.o....[...:~.*.0..1.zf..Y.*.3"...'t...xl./@...zRI#.[}....A.F.. ..:Wy.....LP.+.s.w... w.z\..I.T..k.....LPXG.....D.Lh)...k.^L.BZ.~.y...*..m...1.n.I....K.....8I#.....{.....G2..cB....Xe.9 ...C.....IR.....Y...j. ?/..&. C.Z...n.ah.....G.J...1$...+.B.*I...DI2oS...hY..J+./....G.H.....i.~R&...D2*...P.m.]..I.<..ColXD.P....._p.U.!b&X[.....G.....urE.u..$..;-.~Q..U.N...k. .9.\H....S"..O.r....M.n..!....YX.Jb..:xBU1.<.D.j.....Ac."VK...B..tx.;....p.....G.....#.^.7...sI.....mha.+3..2..`h.....E`K.nb...p.....9..r.y.<..Y_`.h.[.z..Ud.....k.J....h..S."my.....B... J^..[r.f.*.K..l.=K3. .....Np..jZ..>...l.s...O..O...$.I...{.z.ka.....Z..DbI.|..s.)D.sd_*...z.?.Ok?..Z...\d@y9)=.v&..%L.....yN....u.'*.K....vW].>..^....#+..

C:\Users\user\Desktop\QNCYCDFIJJ\ZGGKNSUKOP.mp3.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97385858418915
Encrypted:	false
SSDEEP:	192:xjnuFwDrCl9UCeF58cFUlqcmN2W7SNOlXbgweV+n:0wrClselZmN2DK0wL
MD5:	9DCEB64E009429AF62B508BDF1BB8D25
SHA1:	6B81D5024FDB1456DA785193DB339CB21515560B

C:\Users\user\Desktop\QNCYCDFIJJ\ZGGKNSUKOP.mp3.bCcBDeabea (copy)

SHA-256:	3039B3328ABB02A2EEA135565BB7C044665DBF9352A968F716CA46BC3B86DB0A
SHA-512:	CD077EC64325FA6FA1D35404FF2FB798052485E94F99E4A18846200FD2B99D76DB0B5492C510F491E415043614A3315F041D6B88941EEF2BB1BB83400ED53CDE
Malicious:	false
Preview:	y'..`.bX....T.<..)K:N....APO..p...#k.p...}....SJ..&.....7.....;.....d.5.3.q.{....Z]G[....l.^Q.._.l.....8...*.....k/.~.Y.0../....Sd..>=..KH;.6...Fg..^r.N./GMDm ...Y1...,|A`...X..<. H..Cm....X....i.o....[...:~.*.0..1.zf..Y.*.3"...'t...xl./@...zRl#.[}....A.F.. ..:Wy.....LP.+.s.w... w.z\..l.T..k.....LPXG.....D.Lh)...k.^L.BZ.~.y...*..m...1.n.l....K.....8l#.....{.....G2..cB....Xe.9 ...C.....IR.....Y...j. ?/..&. C.Z...n.ah.....G.J...1$...+.B.*l...DI2oS...hY..J+./....G.H.....i.~R&...D2*...P.m.]..l.<..ColXD.P....._p.U.!b&X[.....G.....urE.u..$..;-.~Q..U.N...k. .9.\H....S"..O.r....M.n..!....YX.Jb..:xBU1.<.D.j.....Ac."VK...B..tx.;....p.....G.....#.^.7...sI.....mha.+3..2..`h.....E`K.nb...p.....9..r.y.<..Y_`.h.[.z..Ud.....k.J....h..S."my.....B... J^..[r.f.*.K..l.=K3. .....Np..jZ..>...l.s...O..O...$.I...{.z.ka.....Z..DbI.|..s.)D.sd_*...z.?.Ok?..Z...\d@y9)=.v&..%L.....yN....u.'*.K....vW].>..^....#+..

C:\Users\user\Desktop\QNCYCDFIJJ\uCLrcwQ_readme_.txt

Process:	C:\Users\user\Desktop\ab.exe
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	3775
Entropy (8bit):	5.733902755295598
Encrypted:	false
SSDEEP:	48:L9k0ZzV7L/vNbXGZULVDgUp4qNiiE6bm1c0rfWejhAe/YAliM3PXnLHrYxgkH69/:L95zhLNbXGZUe7Ka6pU6i9fLrvE69USz
MD5:	48E5A2612CDA2F13A8F5805C4729B202
SHA1:	E1C2C4BF2573F95BD36F04524D97C782D6BED687
SHA-256:	1B7D3016E5D63665C14C4F32119FCD1DFC6E523418BF498545BD5F2B6DD61F4C
SHA-512:	CE6F36F42414951E290A6E84F81A8A96B3200B56385ACCF06EA1DE63B68695A48F45D5BC5F926E02774B107A933A8656B77381D23829DD0FA2B764C8CF657FB3
Malicious:	false
Preview:	-------=== Your network has been infected! ===-------.....********** DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED ********** .....All your documents, photos, databases and other important files have been encrypted and have the extension: .bCcBDeabea.....You are not able to dec rypt it by yourself. But don't worry, we can help you to restore all your files!.....The only way to restore your files is to buy our special software. Only we can give you this s oftware and only we can restore your files!.....We have also downloaded a lot of private data from your network....If you do not contact as in a 3 days we will post info rmation about your breach on our public news website (avaddongun7rngel.onion) and after 7 days the whole downloaded info.....You can get more information on our page, which is located in a Tor hidden network.....How to get to our page...----------

C:\Users\user\Desktop\SQSJKEBWDT.pdf

Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9825890711738445
Encrypted:	false
SSDEEP:	192:iW6ed4PS9NKrabdCZNMAOOkPhj9Mu06OOkQSFxSZV+n:ifJW+WhRvYIm5
MD5:	CD449FC1F57E31C43ED0892AD55C0911
SHA1:	985E98A4753DC101DD091F3729E4D306D46FDE76
SHA-256:	05230D1AD580B9A1F967DC1293D47B8FE33BC74F7B34A85A2D69DDEFFD7CE0A8
SHA-512:	0B369541278EB8821D9F931D683B51F71488F5F5FAFEDBAF7008ACAFE436A0B02FA2C97AC63D6B0CE65D41905CF832F694D8CC626E905F637A4E2FC6D4B9C41
Malicious:	false
Preview:	.Y..B.YR:.....C.y.l..8.a.t.O..bC=...V..3D.....:=9..q.....*....Q..S.].2....F..%..6 uKuu..{n....W.Z.....AZ.|..l.\.=.a.e.....*.....a...3.H.....@g.....D.S.?.0P>..k-.{a...n.B.n...../.x5.hE..f .M...%..T.i...L....J.....?.$..G..e9..Y.....l,]....$...~..4.....b=....aU.`#[.l#e?Pl..*s@#.Y.....^.::W #MF.?OQY$.Fj.....7...nm..1...~-+6.ZZ.C.jJ.4...m].o....._...p(5.~Y.BM....J+n9.=h .....v(1o..y..:.[h~..E[.>....r;.v.q......"B....._.1..10.u8..]......B+R....`_.....gfN..2..U+.j ..af ...E.:...:qv.....h.N....Y...2.PTc....o..,....+..o.q..=.X....(.....R.5....1.....-.~.,{s....N../.5...K.. A.....&.P..... .r..x... .g...q....+{..f....J.....;...{.rF..v...Adp.....h...{.....^.p._.....Ux..-o\Z.....{...g.PM...0.....N.)q....v.BR.v;9....\Wk.Xj.A..m%..uV.5P.....k .5.....G.}..*@w..''..(. .Qq.....@.r....3_.$)y...GY....~x...y.i]..(..}..Z3..F19..z.?kP..Jn.'....)I.F.cQ.....'fz.pm?.;.....r.....3.....a5MUw|#.K..R.wF...*i....]E....".UH.w.L..

C:\Users\user\Desktop\SQSJKEBWDT.pdf.bCcBDeabea (copy)

Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9825890711738445
Encrypted:	false
SSDEEP:	192:iW6ed4PS9NKrabdCZNMAOOkPhj9Mu06OOkQSFxSZV+n:ifJW+WhRvYIm5
MD5:	CD449FC1F57E31C43ED0892AD55C0911
SHA1:	985E98A4753DC101DD091F3729E4D306D46FDE76
SHA-256:	05230D1AD580B9A1F967DC1293D47B8FE33BC74F7B34A85A2D69DDEFFD7CE0A8
SHA-512:	0B369541278EB8821D9F931D683B51F71488F5F5FAFEDBAF7008ACAFE436A0B02FA2C97AC63D6B0CE65D41905CF832F694D8CC626E905F637A4E2FC6D4B9C41
Malicious:	false

C:\Users\user\Desktop\SQSJKEBWDT.pdf.bCcBDeabea (copy)	
Preview:	.Y..B.YR:.....C.y.l..8.a.t.O..bC=...V..3D.....:=9..q.....*....Q..S.].2....F..%..6 uKuu..{n....W.Z.....AZ.|..l.\.=.a.e.....*.....a...3.H.....@g.....D.S.?.0P>..k-.{a...n.B.n...../.x5.hE..f .M...%..T.i...L...J.....?.$..G..e9..Y.....l,]....$...~..4.....b=....aU.`#[.l#e?PI..*s@#.Y.....^.:.W #MF.?OQY$.Fj.....7...nm..1...~-+6.ZZ.C.jJ.4...m].o...._...p(5.~Y.BM....J+n9.=h .....v(1o..y..:.[h~..E[.>....r;.v.q....."B....._.1..10.u8..]......B+R....`_.....gfN..2..U+.j ..af ...E.:...:qv.....h.N....Y...2.PTc....o..,...+..o.q..=.X....(.....R.5....1.....-.~.,{s....N../.5...K.. A.....&.P..... .r..x... .g...q....+{..f....J.....;...{.rF..v...Adp.....h...{.....^.p._.....Ux..-o\Z.....{...g.PM...0.....N.)q....v.BR.v;9....\Wk.XjA..m%..uV.5P.....k .5.....G.}..*@w..".(. .Qq.....@.r....3_.$)y...GY....~x...y.i]..(..}..Z3..F19..z.?kP..Jn.'....)l.F.cQ.....'fz.pm?.;.....r.....3.....a5MUw|#.K..R.wF...*i....]E....".UH.w.L..

C:\Users\user\Desktop\SUAVTZKNFL.pdf	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97801784462802
Encrypted:	false
SSDEEP:	192:+dD0nCHz20HKCr6p47DtMp7bsz5EYRUO0VMQyPcXEecX3H1fLV+n:PATvrXtMp7i5EImVMNcOHHxs
MD5:	35A1C1E18B19CD1D7D9EAE2236F1F48F
SHA1:	833E616EBE2F358A2B62669A52AC714682DD989F
SHA-256:	6CF67F88332E3F09E0C433E074790524D30A0BCDEFD6DDC99B0E1B0ACE618290
SHA-512:	188C5F4E5749AC34CB3EC451DA88090EF697B38E358CEA1B38DAE58F11E1429C269A68A64AD63E5B7079B9FFB14649BF698AEDF56B2635B51864D1DF6430CFF 1
Malicious:	false
Preview:	.f..N.bO).o~P~P.C.2k..@..Z...YZ.f....4g.n.*`.Y).....\..+J.".%..["...$..{1..C....(.G.U.wU.8Qd....h.O...O..).DL.Nd:.Y..A...$~.K.u.1.hG.S1i...|.....;..".'...&3ul...t.D4..{n..la%.....].#.,a _.....*..2.....+.....k...[W..mi)/}.G..ko.....X.I.N..d....\..T.,g.A/.YeB.....M.0.].4..r..s..r..[..x.Kv..."....@.}"..z.....>.g}.....!.....D.;.....q..U....D....&..kr...FdV.dW.6u.#.....3{...(.Qt.E.d. X.*.....(....#E1...?N!...M.-..o..7...K...Z.....>u.?..<.e..$I...B.....;]..q.....#.Nf.....[.1..F.|...K.&&\....V..v....4..M.{...v.r...4...@.a..y&..._|;\D...A..#...|_].....(/.Ez..S.....9...b ..6.&oN..}..w...W3.....x..];@.....s._.i.b..^.D...-....].c.N. .k.Q..5..Hka?.....dV.....f..0....{.z...Ak.q..._.mc....%.:y..B...)|gN^$.}I.K....-.:....tR%....._4...T...D>RY.R..:Ckr...<...s..;\..... .)fL..gWjf.....6l.fB.J..e>.~...P....?XB4.X...*.st..(.....~.....3..D..'....L..e.^...C.....(.?.^....."Xylz6.7.9..LZw..Q$....|.DW.^.P.~...i.....

C:\Users\user\Desktop\SUAVTZKNFL.pdf.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97801784462802
Encrypted:	false
SSDEEP:	192:+dD0nCHz20HKCr6p47DtMp7bsz5EYRUO0VMQyPcXEecX3H1fLV+n:PATvrXtMp7i5EImVMNcOHHxs
MD5:	35A1C1E18B19CD1D7D9EAE2236F1F48F
SHA1:	833E616EBE2F358A2B62669A52AC714682DD989F
SHA-256:	6CF67F88332E3F09E0C433E074790524D30A0BCDEFD6DDC99B0E1B0ACE618290
SHA-512:	188C5F4E5749AC34CB3EC451DA88090EF697B38E358CEA1B38DAE58F11E1429C269A68A64AD63E5B7079B9FFB14649BF698AEDF56B2635B51864D1DF6430CFF 1
Malicious:	false
Preview:	.f..N.bO).o~P~P.C.2k..@..Z...YZ.f....4g.n.*`.Y).....\..+J.".%..["...$..{1..C....(.G.U.wU.8Qd....h.O...O..).DL.Nd:.Y..A...$~.K.u.1.hG.S1i...|.....;..".'...&3ul...t.D4..{n..la%.....].#.,a _.....*..2.....+.....k...[W..mi)/}.G..ko.....X.I.N..d....\..T.,g.A/.YeB.....M.0.].4..r..s..r..[..x.Kv..."....@.}"..z.....>.g}.....!.....D.;.....q..U....D....&..kr...FdV.dW.6u.#.....3{...(.Qt.E.d. X.*.....(....#E1...?N!...M.-..o..7...K...Z.....>u.?..<.e..$I...B.....;]..q.....#.Nf.....[.1..F.|...K.&&\....V..v....4..M.{...v.r...4...@.a..y&..._|;\D...A..#...|_].....(/.Ez..S.....9...b ..6.&oN..}..w...W3.....x..];@.....s._.i.b..^.D...-....].c.N. .k.Q..5..Hka?.....dV.....f..0....{.z...Ak.q..._.mc....%.:y..B...)|gN^$.}I.K....-.:....tR%....._4...T...D>RY.R..:Ckr...<...s..;\..... .)fL..gWjf.....6l.fB.J..e>.~...P....?XB4.X...*.st..(.....~.....3..D..'....L..e.^...C.....(.?.^....."Xylz6.7.9..LZw..Q$....|.DW.^.P.~...i.....

C:\Users\user\Desktop\SUAVTZKNFL.xlsx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.982133728343291
Encrypted:	false
SSDEEP:	192:G9BGLtnEEOP+kPvHm8oblTnHyIP7IihQs+J785q1oxcxV+n:GqLtEDPNm8YlTnSIP7Iij+J785q1oxcu
MD5:	71503B8FAD2224BBBA0DD18F73FE3A63
SHA1:	1816FC21433626A53C83D580BF74459850AB5092
SHA-256:	8D9DDA40D0DD943B7A9955D2F002C9E40DCBDAC08184559C6F62A67EFAAD839A
SHA-512:	580C5FE18D1F20D2966239876B08736D11563E8A17456B3A3E81C47B2EE83E0E4EE3CE76AF41462DBDB5C6D946E78FBEB187A50C407429689CD4F38593D720C
Malicious:	false
Preview:	N5.;..7...b..k.....QB.F.....q...L/_6...q..H%).M..uxa.S/.....5.Q...&..r:..#."@..*F.NYj.....R...$...4)|.,f..].bH.....1@.C.0_.Q?t.a...e...B.Y...X..*:.....+R.n..?...,"..xR.%6.H.~\.....e .....w.lg...AW.0...*lNP..d.jA.3.h..4m..:.....$.4...@g...l7...f77.J...../....y.` .u.@.^....o..Z}M%..-(.G.....^..F.....G.`.P....D.@b.....a... h7....g.m...GXA.u....:.KP..v<.z.P.;.....S..['t`.Q ..~U..g.dX^M].Y$i.$.Z.6....[...W.#.[.s.Xt...L.6..DQ.K.;x..6.W1.....d+u n.a..Q,.....S..\.tT.....R,=..)..~.BE.Dl..P..V..]....&p.HH.....J....qO..&U..Ob@n.g.....j.K.B'%...>..kY.. 'A4YA..j..>u.^...yOr.U...#X....Q.4..s...j.ct0.r.....W.H2o.-.....?..E;....p....9...%[X.Kd$T.O<.....0..&.'./..._"..-...,D..z+.;....\r..k,Rs1..[A.0.k.P4...d....X._..7..+...L./qt....J"J...._MIi..... 11d..".$.0.....iQ5-....._...{l=,6o...B..Py.0.8.....G..h$~.V.M.T.h..X)k...!qrhE.....5.b.....Y.9.....L.(g.|(..}.W...MdY..|.....3M.*.&..D...*.&..R....G.....xu=.....u`/[+R....*..E.?

C:\Users\user\Desktop\SUAVTZKNFL.xlsx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe

C:\Users\user\Desktop\SUAVTZKNFL.xlsx.bCcBDeabea (copy)	
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.982133728343291
Encrypted:	false
SSDEEP:	192:G9BGLtnEEOP+kPvHm8oblTnHyIP7IihQs+J785q1oxcxV+n:GqLtEDPNm8YlTnSIP7Iij+J785q1oxcu
MD5:	71503B8FAD2224BBBA0DD18F73FE3A63
SHA1:	1816FC21433626A53C83D580BF74459850AB5092
SHA-256:	8D9DDA40D0DD943B7A9955D2F002C9E40DCBDAC08184559C6F62A67EFAAD839A
SHA-512:	580C5FE18D1F20D2966239876B08736D11563E8A17456B3A3E81C47B2EE83E0E4EE3CE76AF41462DBDB5C6D946E78FBEB187A50C407429689CD4F38593D720C
Malicious:	false
Preview:	N5.;..7...b..k.....QB.F.....q...L/_6...q..H%).M..uxa.S/.....5.Q...&..r:..#."@..*F.NYj.....R...$...4)\|.f..].bH.....1@.C.0_.Q?t.a...e...B.Y...X..*:.....+R.n..?...,"..xR.%6.H.~\.....e .....w.lg...AW.0...*lNP..d.jA.3.h..4m..:....$.4...@g...l7...f77.J...../....y.` .u.@.^....o..Z}M%..-(.G.....^..F.....G.`.P....D.@b.....a... h7....g.m...GXA.u.....:.KP..v<.z.P.;.....S..['t`.Q ..~U..g.dX^M].Y$i.$.Z.6....[...W.#.[.s.Xt...L.6..DQ.K.;x..6.W1.....d+u n.a..Q,.....S..\.tT.....R,=..)..~.BE.Dl..P..V..]....&p.HH.....J....qO..&U..Ob@n.g.....j.K.B'%...>..kY.. 'A4YA..j..>u.^...yOr.U...#X....Q.4..s...j.ct0.r.....W.H2o.-.....?..E;....p....9...%[X.Kd$T.O<.....0..&.'./.._.",..,..D..z+.;....\r..k,Rs1..[A.0.k.P4...d....X._..7..+...L./qt....J"J...._MIi..... 11d..".$.0.....iQ5-....._...{I=,6o...B..Py.0.8.....G..h$~.V.M.T.h..X)k...!qrhE.....5.b.....Y.9.....L.(.g.|(..}.W...MdY..|.....3M.*.&..D...*.&..R....G.....xu=.....u`/[+R....*..E.?

C:\Users\user\Desktop\ZGGKNSUKOP.mp3	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976858563339414
Encrypted:	false
SSDEEP:	96:lwi7xlVo04wsZ4uMOQ1OzifjR8mLn4lyQ9IEo9TpL/hN5C9b1Fo64WrX6TgamOLg:nwflzi5dxRYRVGZwiJlOS2nyV+n
MD5:	75B41A9884E670E3122B502625945C4F
SHA1:	718309E610BF5A9C9D0FD1A9DA9411527126891B
SHA-256:	8FA89C2D72133BDC3965578D6380A1DE9ECCCEAC7992C9AF4132E994CA7B4BBD
SHA-512:	DAD40B43C22F1A0BBE80CE78BBB9793B58C0988BB208EFC24FCA42B065193E578EF9095F1815C99C1DAF6709D22E41BC1AFF3184D837030CD5DCD2277BFC17B
Malicious:	false
Preview:	q.=.e.'\.4.W.....:3.J...5.....X.5.^...N.6}W.l!..'.%...U.....~hL.X.asl2.....y..}..4....o.....NUP..\.. ...{}.:..&ton.k....?....b..k..;.%%.>IP.{9j....._..m..L.....I.....ZN.v.>2...Q.jz..&_.Ie p.....Y.....t.Zy9:..c..t.J.....x5...g.....V.mi..P.I.....p.....)..N...vs.....t.....ql.....en.k..HCU..j.D:..V.#.f.g..W.)I...$.....X.....C.;....X..Y.....w8.X;..+.....^.]aNH@...M-nu/..m..... ..48F.....24.....1./s..C-.;.V.(<.uC.....m.;.i....Rhx..t.[.#../8....u}4R.R.f....-..3.P..n...,(.r..k@..9c...4.....y.C.....%.sm<...q..C#...OI._N....P...~$.U%.W8.k.~(...?...j..[?`..`..s.g. .$)x.B..e.{....zF3..x...F\|.L..:..=.CUX]h.."~..h6.....)lu"....7^.2.$X..}...!.....1...h..q.p..-.1..Y....].....0N..p..Wm..c....k.l\@.q%+u...k....w>..9...WX.....tx..P.p...!z.pQ8O..G .=....Z..-.v..b.-...a...g..yd.....Q{..r..2..@..G..].!..DK.i+vC.....C.]....<..B/.....b6}..0g.\...=.j..tD./...-.v..dE#..vM...8..._:V..It.$X....)..s..H.

C:\Users\user\Desktop\ZGGKNSUKOP.mp3.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976858563339414
Encrypted:	false
SSDEEP:	96:lwi7xlVo04wsZ4uMOQ1OzifjR8mLn4lyQ9IEo9TpL/hN5C9b1Fo64WrX6TgamOLg:nwflzi5dxRYRVGZwiJlOS2nyV+n
MD5:	75B41A9884E670E3122B502625945C4F
SHA1:	718309E610BF5A9C9D0FD1A9DA9411527126891B
SHA-256:	8FA89C2D72133BDC3965578D6380A1DE9ECCCEAC7992C9AF4132E994CA7B4BBD
SHA-512:	DAD40B43C22F1A0BBE80CE78BBB9793B58C0988BB208EFC24FCA42B065193E578EF9095F1815C99C1DAF6709D22E41BC1AFF3184D837030CD5DCD2277BFC17B
Malicious:	false
Preview:	q.=.e.'\.4.W.....:3.J...5.....X.5.^...N.6}W.l!..'.%...U.....~hL.X.asl2.....y..}..4....o.....NUP..\.. ...{}.:..&ton.k....?....b..k..;.%%.>IP.{9j....._..m..L.....I.....ZN.v.>2...Q.jz..&_.Ie p.....Y.....t.Zy9:..c..t.J.....x5...g.....V.mi..P.I.....p.....)..N...vs.....t.....ql.....en.k..HCU..j.D:..V.#.f.g..W.)I...$.....X.....C.;....X..Y.....w8.X;..+.....^.]aNH@...M-nu/..m..... ..48F.....24.....1./s..C-.;.V.(<.uC.....m.;.i....Rhx..t.[.#../8....u}4R.R.f....-..3.P..n...,(.r..k@..9c...4.....y.C.....%.sm<...q..C#...OI._N....P...~$.U%.W8.k.~(...?...j..[?`..`..s.g. .$)x.B..e.{....zF3..x...F\|.L..:..=.CUX]h.."~..h6.....)lu"....7^.2.$X..}...!.....1...h..q.p..-.1..Y....].....0N..p..Wm..c....k.l\@.q%+u...k....w>..9...WX.....tx..P.p...!z.pQ8O..G .=....Z..-.v..b.-...a...g..yd.....Q{..r..2..@..G..].!..DK.i+vC.....C.]....<..B/.....b6}..0g.\...=.j..tD./...-.v..dE#..vM...8..._:V..It.$X....)..s..H.

C:\Users\user\Desktop\ZQIXMVQGAH.xlsx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977778621685226
Encrypted:	false
SSDEEP:	192:mTbglMUIvyEz2rX/2yQ/SpGfaK6bs08rlO0H6YuPHH4C09RV+n:mvglMUg2HQ/S6aK+E4fNPHd09O
MD5:	23CF59EA3AFE792F21FE4A8C00125E34

C:\Users\user\Desktop\ZQIXMVQGAH.xlsx	
SHA1:	EB403738820421CFA040CA4B1404032788569393
SHA-256:	6C47D734DA1F9817030D14E744D7EBA1C7EC793A86E8713CBCCAB00B907E43B8
SHA-512:	4C01EB5F094A5D9621182D28958F14E1C0E51D5938D9804B2B38D8CE5B8DC3206FBE4F75B504B76B79DC970F0C1AB3FB31BC92286C294D06818C7BDDA4F690
Malicious:	false
Preview:	OqG..k..4Z.5T....H....vA...o.WU...'hE`.P.@.b.S{n..;4...e..S7{.....C.R...0..i.1.pl...a1..h9.i.....w\.....F...R??..Z.u4....B..P.@..z....)a..o.6YC..86..ApW.Bt....3..}.....6..q..4..YY..C.I. -..t.D.GP...1o<'....X{.....=...9....t=TCy...x.m..NF..,..}z....6.%s....*.y><x.y..~C0.....*.].g.N.3.c...G..?Im..D.Z....._..B.x..h...N?.....l]...^.G..5..z.'E.v.....\U.U6b4O..1...B~q...e$., d....2..x..#d..w..@!g..zG..O.5...u.E..Sv.c..^b...k<..B.{.'k.z.;...$.v.6w.o\a.gw.V.5F.~._....0...^.uJ,C.U...@.....y...7.&3L..3.j.....>.....$...$i~.aM).a>9.B..u.(..B.z...<.%.... h w.G+e..y..8$.....%D....l..2.Ht.{%-....<Xj-d...0)/K...a....(..9!....-...!.!..ij.7/....+."....].^...h{p..[.BWM.N..6...$*YU...P.j..:...P.7.aD.,I?G...|.P.lO6T7&.]....7.P.J...N9@...u.I..KS....S. .B.E.&..!.Sq....g.I.. \t..fh..y..... v.gf.D....\..@~..JAM.[. .../<. ...i.+..R.`l....c..]...xS.....k..\.Z.....J`..&..(..Z....8|-.u.&.|."..1..mt..j...1h^.@X.6.p....$+...8^. 7..^!....L..1.....o.|...q.L.#

C:\Users\user\Desktop\ZQIXMVQGAH.xlsx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.977778621685226
Encrypted:	false
SSDEEP:	192:mTbglMUIvyEz2rX/2yQ/SpGfaK6bs08rlO0H6YuPHH4C09RV+n:mvglMUg2HQ/S6aK+E4fNPHd09O
MD5:	23CF59EA3AFE792F21FE4A8C00125E34
SHA1:	EB403738820421CFA040CA4B1404032788569393
SHA-256:	6C47D734DA1F9817030D14E744D7EBA1C7EC793A86E8713CBCCAB00B907E43B8
SHA-512:	4C01EB5F094A5D9621182D28958F14E1C0E51D5938D9804B2B38D8CE5B8DC3206FBE4F75B504B76B79DC970F0C1AB3FB31BC92286C294D06818C7BDDA4F690
Malicious:	false
Preview:	OqG..k..4Z.5T....H....vA...o.WU...'hE`.P.@.b.S{n..;4...e..S7{.....C.R...0..i.1.pl...a1..h9.i.....w\.....F...R??..Z.u4....B..P.@..z....)a..o.6YC..86..ApW.Bt....3..}.....6..q..4..YY..C.I. -..t.D.GP...1o<'....X{.....=...9....t=TCy...x.m..NF..,..}z....6.%s....*.y><x.y..~C0.....*.].g.N.3.c...G..?Im..D.Z....._..B.x..h...N?.....l]...^.G..5..z.'E.v.....\U.U6b4O..1...B~q...e$., d....2..x..#d..w..@!g..zG..O.5...u.E..Sv.c..^b...k<..B.{.'k.z.;...$.v.6w.o\a.gw.V.5F.~._....0...^.uJ,C.U...@.....y...7.&3L..3.j.....>.....$...$i~.aM).a>9.B..u.(..B.z...<.%.... h w.G+e..y..8$.....%D....l..2.Ht.{%-....<Xj-d...0)/K...a....(..9!....-...!.!..ij.7/....+."....].^...h{p..[.BWM.N..6...$*YU...P.j..:...P.7.aD.,I?G...|.P.lO6T7&.]....7.P.J...N9@...u.I..KS....S. .B.E.&..!.Sq....g.I.. \t..fh..y..... v.gf.D....\..@~..JAM.[. .../<. ...i.+..R.`l....c..]...xS.....k..\.Z.....J`..&..(..Z....8|-.u.&.|."..1..mt..j...1h^.@X.6.p....$+...8^. 7..^!....L..1.....o.|...q.L.#

C:\Users\user\Desktop\uCLrcwQ_readme_.txt	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	3759
Entropy (8bit):	5.730136376079227
Encrypted:	false
SSDEEP:	48:L9k0ZzV7L/vNbXGZULVDgUp4qNiiE6bm1c0rfWejhAe/YAliM3PXnLHrYxgkH69x:L95zhLNbXGZUe7Ka6pU6i9fLrvE69USV
MD5:	BC4005FCEBB2809AD1A3FC9BFC770F3A
SHA1:	A8E345EDAAD48C68C4D51500F353A3593BAABC08
SHA-256:	A1CC398783672B546E12D4A5EB5642A7E489A5BBF706456F6E31AF4D23AD6A3B
SHA-512:	5D18730BA64987F6A10704D3360F3AE9BEB55F86F9AFBCA5372440CB53799C3D6A108A6802C943380EB42DEB53FE19332DE75711593284520FEF55198665D76E
Malicious:	false
Preview:	-------=== Your network has been infected! ===-------.....********** DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED ********** .....All your documents, photos, databases and other important files have been encrypted and have the extension: .bCcBDeabea.....You are not able to dec rypt it by yourself. But don't worry, we can help you to restore all your files!.....The only way to restore your files is to buy our special software. Only we can give you this s oftware and only we can restore your files!.....We have also downloaded a lot of private data from your network....If you do not contact as in a 3 days we will post info rmation about your breach on our public news website (avaddongun7rngel.onion) and after 7 days the whole downloaded info.....You can get more information on our page, which is located in a Tor hidden network.....How to get to our page...----------

C:\Users\user\Documents\BNAGMGSPLO.jpg	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.975973249865253
Encrypted:	false
SSDEEP:	192:hmfcT2lws1S5xJwkDAwzOCzkLPbs0xY3Pw6tVbqnPoV+n:KcThs1lwkDAXCzkLwLVbqPx
MD5:	2DF9548BCB84A6887C5F3547B716F2D1
SHA1:	1CA0D7F6A5C83DFB6F70703EFC1CEE73A5D865D0
SHA-256:	FE582B581489E32FAD98813E86B8A2F2C1D0687E28020F80351CC30EA272D3F6
SHA-512:	7CD1131ED325F2595A05B0FC08F5803E26B7162A96F2A5F22FED893691D312361B230E3D736D5C1B2946D3E250642554BB1857427D122C0A408D7A1FE105DAEE
Malicious:	false

C:\Users\user\Documents\BNAGMGSPLO.jpg	
Preview:	apz.)..w....@.....T.C.E...?...H.....l..~Qk.x.Y]:.z8.\...k.e...c{y.A..d.y....*..(L]O.....5.....R.a.&..>*1.....uj..O'.....w...j..T....g..y..Q...zX....$.{'...k\....a,U....."O."?P.....F7...#." 6..3/h..k...G..C...p`.....t@1>G.#.Z[.....u.:.2:.0c.F.p...&t..R.P.....:..n.7.....^!!i+LGo....v...b.y$H9.D];=.K.....B>.x..~..q.....m...`.],,..\(...._0?.8...=Z2....:...JBc.A.C..y.p...Q4.p.. .?..+..F.T.8..i..{D...,.....X.....?.0r....T9:.....'..dc*W..e...@e...d.ve"Fe.8._.....as....<Y#'mT.V{..".D"%.U.=.]..t.F....k..x..."-.?T.0!J5O..s..]RTXA$...C.n.v..Y....*.Y.b.e...(Ou.84 .o..@.+h.~.....E4...=....7....R.E..Q+....B....?...|?cY...K..b.eQJ..d.W.,.xzL...l....tk.....*&_....B..}.....Q.\F.p|q.c.}.:.....@....v!]..X[E..3..G..w....."&}.7.y.5.1..;....Z....{..f.W.i.6%....*. (|..l./.B>..*}-u.....Y.....y...=....B..;x..ul..w.jB.z..f.Z.b^...N.,.M.....m.....V.5).'v....kd.....Z.{F..m.i...F?...=.6M....g.zS:...2....t.j..$.F..'7x..q..

C:\Users\user\Documents\BNAGMGSPLO.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.975973249865253
Encrypted:	false
SSDEEP:	192:hmfcT2lws1S5xJwkDAwzOCzkLPbs0xY3Pw6tVbqnPoV+n:KcThs1IwkDAXCzkLwLVbqPx
MD5:	2DF9548BCB84A6887C5F3547B716F2D1
SHA1:	1CA0D7F6A5C83DFB6F70703EFC1CEE73A5D865D0
SHA-256:	FE582B581489E32FAD98813E86B8A2F2C1D0687E28020F80351CC30EA272D3F6
SHA-512:	7CD1131ED325F2595A05B0FC08F5803E26B7162A96F2A5F22FED893691D312361B230E3D736D5C1B2946D3E250642554BB1857427D122C0A408D7A1FE105DAEE
Malicious:	false
Preview:	apz.)..w....@.....T.C.E...?...H.....l..~Qk.x.Y]:.z8.\...k.e...c{y.A..d.y....*..(L]O.....5.....R.a.&..>*1.....uj..O'.....w...j..T....g..y..Q...zX....$.{'...k\....a,U....."O."?P.....F7...#." 6..3/h..k...G..C...p`.....t@1>G.#.Z[.....u.:.2:.0c.F.p...&t..R.P.....:..n.7.....^!!i+LGo....v...b.y$H9.D];=.K.....B>.x..~..q.....m...`.],,..\(...._0?.8...=Z2....:...JBc.A.C..y.p...Q4.p.. .?..+..F.T.8..i..{D...,.....X.....?.0r....T9:.....'..dc*W..e...@e...d.ve"Fe.8._.....as....<Y#'mT.V{..".D"%.U.=.]..t.F....k..x..."-.?T.0!J5O..s..]RTXA$...C.n.v..Y....*.Y.b.e...(Ou.84 .o..@.+h.~.....E4...=....7....R.E..Q+....B....?...|?cY...K..b.eQJ..d.W.,.xzL...l....tk.....*&_....B..}.....Q.\F.p|q.c.}.:.....@....v!]..X[E..3..G..w....."&}.7.y.5.1..;....Z....{..f.W.i.6%....*. (|..l./.B>..*}-u.....Y.....y...=....B..;x..ul..w.jB.z..f.Z.b^...N.,.M.....m.....V.5).'v....kd.....Z.{F..m.i...F?...=.6M....g.zS:...2....t.j..$.F..'7x..q..

C:\Users\user\Documents\EEGWXUHVUG.png	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.979119574837885
Encrypted:	false
SSDEEP:	192:DmVS9drONMnN1jMaHlRdAHmS/9XDnhkLBiGabHCBYV+n:F6aN1waHlRE/9XDnQBi3iBB
MD5:	432F844E78E55603BCF423CED2F41FD3
SHA1:	3B2BC3C7419EB461FAAEDC085D0E6141AE9D9D65
SHA-256:	7FB2181204E0DF582D73A87710DC820244FC811CFBEFABF4E3F2A238A889A932
SHA-512:	5EA8FE8D4A9DB997BAD9DC9F53FACABC693FC781D3B167E6E47651AC072CB7C708B2CD9B83C729DC48030D9A1A325652D07ED938D4ACC83860EE629DDD81F94
Malicious:	false
Preview:	%UYG.!....az.}o..m6...o }...DY..&.....'.4...q.BZPn-(.E%@..4..WR.rR..L...V..5..../g..:....Dh!j1..r'.....D.....^....e55...s.b;!.....a.....$.|.....,L...Gu.@JB.j2~...+.6..... .abt. .E...D..n.#.....*.RAC...8Oi.%M(....f..P..)...Yn.\.R9.~.Gj..v.....]...Ed+{.^...j.Y.....~ ....=...n..}I.G.kGS.....}.W._.0U|.1.a...W..f.gU..9.#.n.ZC..w.R'....F1..u....~K.q#.D:..G(...c ;.),#x.....[.ip.....S....C..9....j.0\'.....b.N.j..G....0.....h...D...H..d^....A.b.=.<v.{1..U.O3..Pj{u.....Hw.W.`.....Fk.!.7..7.....a.f)b..r...q+Av...c.nJ.M9..n.mF..y.....a..F.....9J..... \P..Dh X4..}.o..`...,3.K<5jZ..#..... .....q.x.....Q....J...1.dUxj.5Y.(.QYK...U.....S.....{./...]....P!~.....?[.U...&7..W...d..V3.&Yo..4./B.v.0..C.=..v.PpF...k....n..=....n~.....Ui.....C5./\ ...Ga.....12.e.....W....Vj.-.Dt. .U]..hI..(.8.D...?ThaJ.....*s2k.m!zs*z[..>~...,]...2..F.ayr...hG. a|4..4k...=K...o...(Ujtm=....3$.%.....Uq.+e[..=.Q.j$.7..1..

C:\Users\user\Documents\EEGWXUHVUG.png.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.979119574837885
Encrypted:	false
SSDEEP:	192:DmVS9drONMnN1jMaHlRdAHmS/9XDnhkLBiGabHCBYV+n:F6aN1waHlRE/9XDnQBi3iBB
MD5:	432F844E78E55603BCF423CED2F41FD3
SHA1:	3B2BC3C7419EB461FAAEDC085D0E6141AE9D9D65
SHA-256:	7FB2181204E0DF582D73A87710DC820244FC811CFBEFABF4E3F2A238A889A932
SHA-512:	5EA8FE8D4A9DB997BAD9DC9F53FACABC693FC781D3B167E6E47651AC072CB7C708B2CD9B83C729DC48030D9A1A325652D07ED938D4ACC83860EE629DDD81F94
Malicious:	false
Preview:	%UYG.!....az.}o..m6...o }...DY..&.....'.4...q.BZPn-(.E%@..4..WR.rR..L...V..5..../g..:....Dh!j1..r'.....D.....^....e55...s.b;!.....a.....$.|.....,L...Gu.@JB.j2~...+.6..... .abt. .E...D..n.#.....*.RAC...8Oi.%M(....f..P..)...Yn.\.R9.~.Gj..v.....]...Ed+{.^...j.Y.....~ ....=...n..}I.G.kGS.....}.W._.0U|.1.a...W..f.gU..9.#.n.ZC..w.R'....F1..u....~K.q#.D:..G(...c ;.),#x.....[.ip.....S....C..9....j.0\'.....b.N.j..G....0.....h...D...H..d^....A.b.=.<v.{1..U.O3..Pj{u.....Hw.W.`.....Fk.!.7..7.....a.f)b..r...q+Av...c.nJ.M9..n.mF..y.....a..F.....9J..... \P..Dh X4..}.o..`...,3.K<5jZ..#..... .....q.x.....Q....J...1.dUxj.5Y.(.QYK...U.....S.....{./...]....P!~.....?[.U...&7..W...d..V3.&Yo..4./B.v.0..C.=..v.PpF...k....n..=....n~.....Ui.....C5./\ ...Ga.....12.e.....W....Vj.-.Dt. .U]..hI..(.8.D...?ThaJ.....*s2k.m!zs*z[..>~...,]...2..F.ayr...hG. a|4..4k...=K...o...(Ujtm=....3$.%.....Uq.+e[..=.Q.j$.7..1..

C:\Users\user\Documents\EFOYFBOLXA.jpg	
Process:	C:\Users\user\Desktop\ab.exe

C:\Users\user\Documents\EFOYFBOLXA.jpg	
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9781551548759015
Encrypted:	false
SSDEEP:	192:EkYONEeDIJcTErEnsgQhgF6K8dSPDFl1WLJkLkudkc8BdvwV+n:EkYONEe2cTpm2EHdSLZWCeRL
MD5:	06654039C5F933CFA2EEC4D750A74DF5
SHA1:	026FF645FAB17FF0CFBD0F372840119E952FAAB2
SHA-256:	B370F2648964D4AFB50C6EFB10068910088AF3811BB6E501B5D5F6248C346120
SHA-512:	8A4FBCA824A6C0931ECE1A1CD4A7963F9681A3FEE2DF36E1F6D25DAFD8354606C18756242B90C25AF40D66AEBD7D387B9FE9A6D9892A0BA81309F71154EB95C
Malicious:	false
Preview:	....!..... ..y}*.K..L.W7X..:...!T..Y!.0...]G......o...F.J.[W@c.....i.n..B...I.W.t<B..a.b_h9.Z..E.7.uN-a9c...|g...>..]..... N...6.oa..87.,...AA..s.....63.k.....#....r6.....w.....n....Le.....s. v....5..n.....&..[.&.^..Q.....}...{.....+..*2`...T..[...dbr...+. .&p.I....''..N.>PCn..1'.....F.s.5...Z.....KM,s.Q....|.4.....c...L..4EG..Z..W..0...w.....2.2._...L+j..._@...b.S.a...5O .>9.*...z...D...vr.T4...@PYf....c..>...,Gb.1.W.j...nR>..{).....:..{.6.c0..^.....=.....5...=..e.*.....'!>..$+=.....X.jjD.e....Y..&9.u..a.0]..hJ.v.....#.<xu..[...X....b.%....y.....B.] 'W...m..C.....-....Uzd....4....n.e+.0....}..%..._...Y.....y....>.S.>...UJ.....*p...h>w..r...*.>]].Gm.R.....(.....IzB...#..<B.D*jG+J..[.n..^....f..,g.....-Ss....9/F..?._<.....0..{..,..=...6[.M...}.. .`.....H.R...%x..1...).v..+A....<.....U.....JdYb.\..<..7Tk ./*o.D;.....;.5..i...v..7Y}....'...xk...y...'f.j/..a.F...|

C:\Users\user\Documents\EFOYFBOLXA.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9781551548759015
Encrypted:	false
SSDEEP:	192:EkYONEeDIJcTErEnsgQhgF6K8dSPDFl1WLJkLkudkc8BdvwV+n:EkYONEe2cTpm2EHdSLZWCeRL
MD5:	06654039C5F933CFA2EEC4D750A74DF5
SHA1:	026FF645FAB17FF0CFBD0F372840119E952FAAB2
SHA-256:	B370F2648964D4AFB50C6EFB10068910088AF3811BB6E501B5D5F6248C346120
SHA-512:	8A4FBCA824A6C0931ECE1A1CD4A7963F9681A3FEE2DF36E1F6D25DAFD8354606C18756242B90C25AF40D66AEBD7D387B9FE9A6D9892A0BA81309F71154EB95C
Malicious:	false
Preview:	....!..... ..y}*.K..L.W7X..:...!T..Y!.0...]G......o...F.J.[W@c.....i.n..B...I.W.t<B..a.b_h9.Z..E.7.uN-a9c...|g...>..]..... N...6.oa..87.,...AA..s.....63.k.....#....r6.....w.....n....Le.....s. v....5..n.....&..[.&.^..Q.....}...{.....+..*2`...T..[...dbr...+. .&p.I....''..N.>PCn..1'.....F.s.5...Z.....KM,s.Q....|.4.....c...L..4EG..Z..W..0...w.....2.2._...L+j..._@...b.S.a...5O .>9.*...z...D...vr.T4...@PYf....c..>...,Gb.1.W.j...nR>..{).....:..{.6.c0..^.....=.....5...=..e.*.....'!>..$+=.....X.jjD.e....Y..&9.u..a.0]..hJ.v.....#.<xu..[...X....b.%....y.....B.] 'W...m..C.....-....Uzd....4....n.e+.0....}..%..._...Y.....y....>.S.>...UJ.....*p...h>w..r...*.>]].Gm.R.....(.....IzB...#..<B.D*jG+J..[.n..^....f..,g.....-Ss....9/F..?._<.....0..{..,..=...6[.M...}.. .`.....H.R...%x..1...).v..+A....<.....U.....JdYb.\..<..7Tk ./*o.D;.....;.5..i...v..7Y}....'...xk...y...'f.j/..a.F...|

C:\Users\user\Documents\EFOYFBOLXA.mp3	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976427242589434
Encrypted:	false
SSDEEP:	192:nUCyyCchlWapf9fHToARU0wrVoz6gH8y4zCJGrpGm1JIErvfU9V+n:UCJ1hl5FEOsrO6g4zeGT1J1H3
MD5:	20CBF10010208A2F4D0B291E62757E1E
SHA1:	5B7CDD890C01F28F35E77005991B3E7A2C4C83E2
SHA-256:	AED905F09E4E1F08EEB5B3DFBDBCEBCEA064DF7D5F14C97A09DE9C9C3EDF49E1
SHA-512:	9033F01D3DC0D872547249C9E8FA5C6664D24167ACBAFB42E29212DFF06BE0AA6F3C1F907138C907CF6380482B3EA50A5495A0318DDCDC4B17C9325EB60DA3
Malicious:	false
Preview:	.h8.d@...:..V..H7 "..R.@k.....I.X....).g..6.....I...;wF..zV......S......Ru.....-7.^....j}d.=C.q.....~.G...1..7.w$5Om.(.r.@....\|.}.I...Qi..t.=.g.....s..h..L,+.H'.8^..f.mJN.>#Gk.....K.MXMy. ...$..>=.,...&^.....;$b#.s.C.\31..p#.c3.f.jK7.{s...I....dZFpP.6.zn..W'm.....g{!..W..z..f%.....{.>........5..Gd.U?.....".../...].....j...s.....*.Coy....U{4:N.M.N.....Un.....K....^....\|..lb.. ..r..%..c..59.]F...A..$.'.$.I.&i.\|.....y...>`.#?...W.Ur.....'J...{....V.8.:T..C...v....F..AZ...h..xO.:ju.....>..F>..t.t..7oV.j...p.>fm..o.p.H...X.ms....T..1.?.xN"cy..Fy&u.@..q.pd../..k. ....om/Z.h..-...y.A2%54.....&..}.[4).....a.r.w...,.q&V.8!.....sX.....>.Bua<.J...f.....+.#FOP.%$....mU.F....7..uy..9.....k....sw....y&P.P....>S.....K...6{._.x..-ux!1..%..a&.&...G....d0{ .z:|.j9.F.A..|..C..;./..m-a...E....."fa.|..s<4Y.....-.r...X.u.....ZP..[.M.u'..D..+.Ew..US.ms....o<.b..G.t..?N.Y9.>..G...z..*..h..}.`. .e.]...}.;*.Z"."yX.....>EN..!k...<A.%.

C:\Users\user\Documents\EFOYFBOLXA.mp3.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976427242589434
Encrypted:	false
SSDEEP:	192:nUCyyCchlWapf9fHToARU0wrVoz6gH8y4zCJGrpGm1JIErvfU9V+n:UCJ1hl5FEOsrO6g4zeGT1J1H3
MD5:	20CBF10010208A2F4D0B291E62757E1E

C:\Users\user\Documents\EFOYFBOLXA.mp3.bCcBDeabea (copy)	
SHA1:	5B7CDD890C01F28F35E77005991B3E7A2C4C83E2
SHA-256:	AED905F09E4E1F08EEB5B3DFBDBCEBCEA064DF7D5F14C97A09DE9C9C3EDF49E1
SHA-512:	9033F01D3DC0D872547249C9E8FA5C6664D24167ACBAFB42E29212DFF06BE0AA6F3C1F907138C907CF6380482B3EA50A5495A0318DDCDC4B17C9325EB60DA3
Malicious:	false
Preview:	.h8.d@...:..V..H7 "..R.@k.....I.X....).g..6....l...;wF..zV.....S......Ru.....-7.^....j}d.=C.q.....~.G...1..7.w$5Om.(.r.@....|.}.I...Qi..t.=.g.....s..h..L,+.H'.8^..f.mJN.>#Gk.....K.MXMy. ...$..>=,,...&^.....;$b#.s.C.\31..p#.c3.f.jK7.{s...l....dZFpP.6.zn..W'm.....g{!..W..z..f%....{.>.....5..Gd.U?....."../...]......j...s.....*.Coy....U{4:N.M.N.....Un.....K....^....|..Ib.. ..r..%..c..59.]F...A..$.'.$.I.&.i.|.....y...>`.#?...W.Ur.....'J...{....V.8.:T..C...v....F..AZ...h..xO.:ju.....>..F>..t.t..7oV.j...p.>fm..o.p.H...X.ms....T..1.?.xN"cy..Fy&u.@..q.pd../..k. ....om/Z.h..-...y.A2%54.....&..}.[4).....a.r.w...,.q&V.8!.....sX.....>.Bua<.J...f.....+.#FOP.%$....mU.F....7..uy..9.....k....sw....y&P.P....>S.....K...6{._.x..-ux!1..%..a&.&...G....d0{ .z:|.j9.F.A..|..C..;./..m-a...E....."fa.|..s<4Y.....-.r...X.u.....ZP..[.M.u'..D..+.Ew..US.ms....o<.b..G.t..?N.Y9.>..G...z..*..h..}.`. .e.]...}.;*.Z"."yX.....>EN..!k...<A.%.

C:\Users\user\Documents\GAOBCVIQIJ.docx	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	DOS executable (COM, 0x8C-variant)
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9774485548647185
Encrypted:	false
SSDEEP:	192:DlRAdYaiKM9AyTan0q0pbGddw91P2vl8005mV+n:xHaiKM9LTo0q0pCdmHP2SjV
MD5:	6A8B803018F15DF09E956F0452506416
SHA1:	DBBB7284D7CE111DDBA9BF384A64DBC13E13E1E9
SHA-256:	45369EC2F9CC5C35957892C3BD991CF9C0AA6CC128E46D09AB79EA61765476E6
SHA-512:	98D012E161745993DD2DA6CF40BDE589AB8A8602338991E005CBE72E271AE970F5C5739C22C35F027D4D94167BEAB129DC63E8D389F0E1B67F66997686144239
Malicious:	false
Preview:	...4...GQ.....=HLHe.xg...pTMUfL>.#L....Z....[...../...rk.3.m.B%.....K...+Y.[...."....N.....WcL}G.\.F5.?..nR.^..V..h'..#.~|[.9.D.h.^z.opf.)A.YnN.;-.(.....V.l....c.B..j...f*Fx...iO..!rM. S.....qa..2@bt.)...,...._...@...3.Us.i...O....^.......N.....8GK.....A...,.....dG.GF.N...s..A:'8Hv=...,.e.....S.....mJ.-...<t.4.....p.+<;<...b..|u-1..+.....Q.....b...|..'.c.owD..... ...&.Nn{^...~a...}`._T..8.Bc.+.)B...Q.|..Kt.%9.....r..m%.&..X...3.^.H..T.R.r`....z.._...r..>...Id.....Q.+*..|.;.r....q.D....A@.`8.Pc<5....D.6.|6...5.j..!....!1.....(..p5..h.. .2+.!.(..... ..%S[..>.'.2.....I...?....;...,.w.O....2..`..qcr.l..jX..f`;.H.~U.<.t....7Y.`.J...{..d...1.....g..n..z.bI...Z.....~x..8....6.nr...t..8)..|Z..Q..)`....^|.8U~5....k.....V...{.P...,.^...Z...R..SS..\...[.P}..I .....l#.#PAvu..J.'egg.`5...{.:Dj.k.6..I1.(.n....`..4*.i...}...0...aLH.Pi..9N.[9.c.m}....)...4B.....[..b.....!k.....l...<D.=:...w..)#....3.C

C:\Users\user\Documents\GAOBCVIQIJ.docx.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	DOS executable (COM, 0x8C-variant)
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9774485548647185
Encrypted:	false
SSDEEP:	192:DlRAdYaiKM9AyTan0q0pbGddw91P2vl8005mV+n:xHaiKM9LTo0q0pCdmHP2SjV
MD5:	6A8B803018F15DF09E956F0452506416
SHA1:	DBBB7284D7CE111DDBA9BF384A64DBC13E13E1E9
SHA-256:	45369EC2F9CC5C35957892C3BD991CF9C0AA6CC128E46D09AB79EA61765476E6
SHA-512:	98D012E161745993DD2DA6CF40BDE589AB8A8602338991E005CBE72E271AE970F5C5739C22C35F027D4D94167BEAB129DC63E8D389F0E1B67F66997686144239
Malicious:	false
Preview:	...4...GQ.....=HLHe.xg...pTMUfL>.#L....Z....[...../...rk.3.m.B%.....K...+Y.[...."....N.....WcL}G.\.F5.?..nR.^..V..h'..#.~|[.9.D.h.^z.opf.)A.YnN.;-.(.....V.l....c.B..j...f*Fx...iO..!rM. S.....qa..2@bt.)...,...._...@...3.Us.i...O....^.......N.....8GK.....A...,.....dG.GF.N...s..A:'8Hv=...,.e.....S.....mJ.-...<t.4.....p.+<;<...b..|u-1..+.....Q.....b...|..'.c.owD..... ...&.Nn{^...~a...}`._T..8.Bc.+.)B...Q.|..Kt.%9.....r..m%.&..X...3.^.H..T.R.r`....z.._...r..>...Id.....Q.+*..|.;.r....q.D....A@.`8.Pc<5....D.6.|6...5.j..!....!1.....(..p5..h.. .2+.!.(..... ..%S[..>.'.2.....I...?....;...,.w.O....2..`..qcr.l..jX..f`;.H.~U.<.t....7Y.`.J...{..d...1.....g..n..z.bI...Z.....~x..8....6.nr...t..8)..|Z..Q..)`....^|.8U~5....k.....V...{.P...,.^...Z...R..SS..\...[.P}..I .....l#.#PAvu..J.'egg.`5...{.:Dj.k.6..I1.(.n....`..4*.i...}...0...aLH.Pi..9N.[9.c.m}....)...4B.....[..b.....!k.....l...<D.=:...w..)#....3.C

C:\Users\user\Documents\GAOBCVIQIJ.pdf	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976281289227903
Encrypted:	false
SSDEEP:	192:n1onrqTYRauwhprNWHWJW712a6ElZKu/V+n:n1or2NW2AZho
MD5:	A6FC66F9031DAAB2F274CDD29D76E78C
SHA1:	4223A091E1ED2AF160C2A7B29E8CEE79D1050036
SHA-256:	1FEC9CE17438CF44B3EF047512CFDBB73D49A45A70FFFC8DC1F7214C9264F9D1
SHA-512:	A084E42725D3A4DB848BA27EC139977DBE1EF373395D10597178A62C1D9DB31A04E47286AB80FBFAA9BA51B022760103092D0F03801285B21B3F54B3704FB74F
Malicious:	false
Preview:	..h.:....s|3+...3...Kt.k....T....ldKMs.K...G.-9.}.1|$.P...F.@..o..].X,.u.k.....3..J8D..~..E.?.....C..1.K..T...^...fDq..../...h...n...a...B..6.LE...>Q.....\|].S\E}..AD.X..J..*>-<P..$FM..V`.r6. ....o..".=.t..'[.$.P. ?.h..s.O$..7%..=..h...@....9]....~.vU..;.<.....`8M2.V#'GS.\..1....8....v!..6..4k..[...xS..]...+{|...i...HO.GOo....b.D..?..._..w.....;....4.SC*q..X.M.R.:..e.{W.UU..x..5..? L5...178_e.....pM...< mP....."....|9i..3.E?.Siv..Jy#.7.\\...j.X..~.....+....f.....U.....@.k5(T..iM.....$..i{.....[.....H..\|y....p...N.5..q!j.3..$j..t..x.7e...?.U*...Cz...R.....Z....?.iw..H....>.]..eI, 7Q..f..gH.4.:K.&....ex`..g.....6....>1\'.T.Ss+.a..o1...)..5. L2..C.<g...O...kj..r....)9:.=~!.#|..|...AL..I...x..)5...se.. ...6J..f..1{(d].1.4zUW~"S|. .o9....J..f.....`s.....VK...V....':...3... ..HhZ..RI.....t6.o...^.W....%D....?.o...l..U u..NhiS.....BN.-.ds....5.i....,x....kD...../.....i).iQ.E.$....Jy.U....B.~nf..-.G2R.dsU..Y..cF

C:\Users\user\Documents\GAOBCVIQIJ.pdf.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.976281289227903
Encrypted:	false
SSDEEP:	192:n1onrqTYRauwhprNWHWJW712a6ElZKu/V+n:n1or2NW2AZho
MD5:	A6FC66F9031DAAB2F274CDD29D76E78C
SHA1:	4223A091E1ED2AF160C2A7B29E8CEE79D1050036
SHA-256:	1FEC9CE17438CF44B3EF047512CFDBB73D49A45A70FFFC8DC1F7214C9264F9D1
SHA-512:	A084E42725D3A4DB848BA27EC139977DBE1EF373395D10597178A62C1D9DB31A04E47286AB80FBFAA9BA51B022760103092D0F03801285B21B3F54B3704FB74F
Malicious:	false
Preview:	..h.:....s|3+...3...Kt.k....T....ldKMs.K...G.-9.}.1|$.P...F.@..o..].X,.u.k.....3..J8D..~..E.?.....C..1.K..T...^...fDq..../...h...n...a...B..6.LE...>Q.....\|].S\E}..AD.X..J..*>-<P..$FM..V`.r6. ....o..''=.t..'[.$.P. ?.h..s.O$..7%..=..h...@....9]....~.vU..;.<.....`8M2.V#'GS.\..1....8....v!..6..4k..[...xS..]...+{|...i...HO.GOo....b.D..?..._..w.....;....4.SC*q..X.M.R.:..e.{W.UU..x..5..? L5...178_e.....pM...< mP.....''....|9i..3.E?.Siv..Jy#.7.\\...j.X..~.....+....f.....U.....@.k5(T..iM.....$..i{.....[.....H..\|y....p...N.5..q!j.3..$j..t..x.7e...?.U*...Cz...R.....Z....?.iw..H....>.]..eI, 7Q..f..gH.4.:K.&....ex`..g......6....>1\'.T.Ss+.a..o1...)..5. L2..C.<g...O...kj..r....)9:.=~!.#|..|...AL..I...x..)5...se.. ...6J..f..1{(d].1.4zUW~''S|. .o9....J..f.....`s.....VK...V....':...3... ..HhZ..RI.....t6.o...^.W....%D....?.o...l..U u..NhiS.....BN.-.ds....5.i....,x....kD...../.....i).iQ.E.$....Jy.U....B.~nf..-.G2R.dsU..Y..cF

C:\Users\user\Documents\GAOBCVIQIJ\BNAGMGSPLO.jpg	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978580903469927
Encrypted:	false
SSDEEP:	192:KqIsl3ttRIjiryxEuk2r0SzCzzQy2BzjEFetuV+n:KqI0RIgqEuk2fz+N2Bz4FG7
MD5:	26554AD741CD3BB34D9BE63A4609CB78
SHA1:	8F9C143F1E42E68A3BDED3CF5107DB5ED2C6C861
SHA-256:	E1ED686D36969596D39A9B8E0F6A6B88A46E3A7F56FBCB68C5A46BE8B5E7B9DF
SHA-512:	8AB405CEF2846D5BEC06E0D846AB2EFEEE6C509EEC7E05A4BB7A3679D4FAF7B61693036358608D20C022280CC392133F5038E0C7DC01D0B6AE762024E217551
Malicious:	false
Preview:	...I...i.....].U...~...O<...hV.....X.'D...7@|.E...3._....w./...S&>.)._..k.b..]..3..H..R.0=`-..c.Dz.z....W.I;oLB..0..y..l.x<.....2.........\.-.8...N&.....o.t.eT.2.i...xz;;...a.p..jC.P$y:,QM x..HyD.J.}.#...a.mg{....M4...^...}....V.[z.v.6.9..rK...cv4...A.A...ee.9^s.....lfQ.....?.^.?.c.W..b..j..k3...W.....%.....hqW...K.....z.lm..hF...x..K.q!.a...:...NXm.}R..2D-..^I...^FdU..... *.U...OT..D_py..... ._.i.0."a~`.~...&=.h....`.x.& ...dduA.p$9 VD..C.Oc:..:z.i.....,..QQ..qIt.....K.....'.7..H..\...F..;I...1.O...rf..&....._.s..Q..}oTr.w...,...M<.t...Q..U..$DKV....Ok J.q.....L..S..nY....^:'.*.....5.....A.<.0....&X.....a.;..8.|.I5..._..(.Z.P.V..L..m...<3.._.`D.?.....F.Z.-q...4.P=....5.#...C._...U...H....n...+**vtbC$.....a....5.`.N.%.w,M.'.....t%3rt....t*'.. <.1..y.9(0TXN6.y.''.~.%Ow.X....D.3.E.H.U.~...aC.Q....kw.]..j.*....T.^.....$...99J.....kL.....d...c....M..4...z..t1.4/IVR.9.V@.C.$...<t.....E.o(..`.+.....(.!....t...4y

C:\Users\user\Documents\GAOBCVIQIJ\BNAGMGSPLO.jpg.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.978580903469927
Encrypted:	false
SSDEEP:	192:KqIsl3ttRIjiryxEuk2r0SzCzzQy2BzjEFetuV+n:KqI0RIgqEuk2fz+N2Bz4FG7
MD5:	26554AD741CD3BB34D9BE63A4609CB78
SHA1:	8F9C143F1E42E68A3BDED3CF5107DB5ED2C6C861
SHA-256:	E1ED686D36969596D39A9B8E0F6A6B88A46E3A7F56FBCB68C5A46BE8B5E7B9DF
SHA-512:	8AB405CEF2846D5BEC06E0D846AB2EFEEE6C509EEC7E05A4BB7A3679D4FAF7B61693036358608D20C022280CC392133F5038E0C7DC01D0B6AE762024E217551
Malicious:	false
Preview:	...I...i.....].U...~...O<...hV.....X.'D...7@|.E...3._....w./...S&>.)._..k.b..]..3..H..R.0=`-..c.Dz.z....W.I;oLB..0..y..l.x<.....2.........\.-.8...N&.....o.t.eT.2.i...xz;;...a.p..jC.P$y:,QM x..HyD.J.}.#...a.mg{....M4...^...}....V.[z.v.6.9..rK...cv4...A.A...ee.9^s.....lfQ.....?.^.?.c.W..b..j..k3...W.....%.....hqW...K.....z.lm..hF...x..K.q!.a...:...NXm.}R..2D-..^I...^FdU..... *.U...OT..D_py..... ._.i.0."a~`.~...&=.h....`.x.& ...dduA.p$9 VD..C.Oc:..:z.i.....,..QQ..qIt.....K.....'.7..H..\...F..;I...1.O...rf..&....._.s..Q..}oTr.w...,...M<.t...Q..U..$DKV....Ok J.q.....L..S..nY....^:'.*.....5.....A.<.0....&X.....a.;..8.|.I5..._..(.Z.P.V..L..m...<3.._.`D.?.....F.Z.-q...4.P=....5.#...C._...U...H....n...+**vtbC$.....a....5.`.N.%.w,M.'.....t%3rt....t*'.. <.1..y.9(0TXN6.y.''.~.%Ow.X....D.3.E.H.U.~...aC.Q....kw.]..j.*....T.^.....$...99J.....kL.....d...c....M..4...z..t1.4/IVR.9.V@.C.$...<t.....E.o(..`.+.....(.!....t...4y

C:\Users\user\Documents\GAOBCVIQIJ\EEGWXUHVUG.png	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9808293019820775
Encrypted:	false
SSDEEP:	192:XwWsIdBAI2rNNREeye0AnNsWXrrJsbyQtTM5/ooaQtkKx+PHmkTcWdkFyV+n:XwWDARV5IFW7YjtQ2bE49/d0
MD5:	9D389747B493661E916D84F0296B4905
SHA1:	3D288034A6A9BFD7CA252878A8679290FCF48EA6

C:\Users\user\Documents\GAOBCVIQIJ\EEGWXUHVUG.png	
SHA-256:	5B91DC3C680A0BFB917C05491AE84DB83718D50762CBAE9BADDC72D27AE528B1
SHA-512:	C2DB72E941C53D6FB189A0681DE4E098A1EA4FBA9AEA7FD550D84C47B7260D9AFD8F708B5A426F6ADBF2D9AE3AE58137757A3E09AD803C9903B8E8675ECF5133
Malicious:	false
Preview:	.)>N....6S.&]......I.I.~lE..H..h.V.L.p[.[.@...r....6K.>.w....<.....`..vC+*O..........S9.].q`P..<$...Z..$.+.rpa*.@.A.@...Z.......%...........G$.a.<...NO.....g.....r......G-i.Z.at`.l.].L.. ..m .T.H.6..eN........@.....,..."..F.Qm.a..F.a .....a....5...TX.X.U$L.ay.w..1.heu.:.....U..f`...t._.L..E.D ..T........./z.9_...Y..........=..7.^f<...'./.......(Cj.b..?m ..`c.k.z].Q.....B......e....;...F... @/.u..gv......[P.....1O.7..-...Vr.......[H...........>.~.F.... .$.........O..J.....7.].).H.1):...l07LB...Z..DGbgW}.i{.$B<.~...2G.G..V!.@k#.....x`.4.....l.d.h.BT.....zt.....)..8..+.')7K.a.......k.... v.+`...e..q._C.....p...Ksl..M.jKU<9...4....&... 1.%9.W. P.L..k(Q_.....9.O.............g.7.SaA.qn.9m.........?.....H...<.B..4............^5#.H.{3.{.DM......8^6-.....!.....$........H...`F....EN.....3.. Zo...u.z.1u/T7....|m^.....q....d.....BR.[|b...f!.V..'.W#VL....._:{!...e."...L...>.M4[.rE.{.E.{.7..n...I...1.....Lo.N.p).Iw.7.L.....YB%..Oa...[.X...

C:\Users\user\Documents\GAOBCVIQIJ\EEGWXUHVUG.png.bCcBDeabea (copy)	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.9808293019820775
Encrypted:	false
SSDEEP:	192:XwWsIdBAI2rNNREeye0AnNsWXrrJsbyQtTM5/ooaQtkKx+PHmkTcWdkFyV+n:XwWDARV5IFW7YjtQ2bE49/d0
MD5:	9D389747B493661E916D84F0296B4905
SHA1:	3D288034A6A9BFD7CA252878A8679290FCF48EA6
SHA-256:	5B91DC3C680A0BFB917C05491AE84DB83718D50762CBAE9BADDC72D27AE528B1
SHA-512:	C2DB72E941C53D6FB189A0681DE4E098A1EA4FBA9AEA7FD550D84C47B7260D9AFD8F708B5A426F6ADBF2D9AE3AE58137757A3E09AD803C9903B8E8675ECF5133
Malicious:	false
Preview:	.)>N....6S.&]......I.I.~lE..H..h.V.L.p[.[.@...r....6K.>.w....<.....`..vC+*O..........S9.].q`P..<$...Z..$.+.rpa*.@.A.@...Z.......%...........G$.a.<...NO.....g.....r......G-i.Z.at`.l.].L.. ..m .T.H.6..eN........@.....,..."..F.Qm.a..F.a .....a....5...TX.X.U$L.ay.w..1.heu.:.....U..f`...t._.L..E.D ..T........./z.9_...Y..........=..7.^f<...'./.......(Cj.b..?m ..`c.k.z].Q.....B......e....;...F... @/.u..gv......[P.....1O.7..-...Vr.......[H...........>.~.F.... .$.........O..J.....7.].).H.1):...l07LB...Z..DGbgW}.i{.$B<.~...2G.G..V!.@k#.....x`.4.....l.d.h.BT.....zt.....)..8..+.')7K.a.......k.... v.+`...e..q._C.....p...Ksl..M.jKU<9...4....&... 1.%9.W. P.L..k(Q_.....9.O.............g.7.SaA.qn.9m.........?.....H...<.B..4............^5#.H.{3.{.DM......8^6-.....!.....$........H...`F....EN.....3.. Zo...u.z.1u/T7....|m^.....q....d.....BR.[|b...f!.V..'.W#VL....._:{!...e."...L...>.M4[.rE.{.E.{.7..n...I...1.....Lo.N.p).Iw.7.L.....YB%..Oa...[.X...

C:\Users\user\Documents\GAOBCVIQIJ\EFOYFBOLXA.mp3	
Process:	C:\Users\user\Desktop\ab.exe
File Type:	data
Category:	dropped
Size (bytes):	8728
Entropy (8bit):	7.97996259530454
Encrypted:	false
SSDEEP:	192:ZvG31SaR6Yni+msLxZ0FzkTQCvkf637vIEah5Dj0a4z2Q6V+n:RkU+msLxuFzkRvkAvIEahS8Q/
MD5:	C39FA9042CAB3AC36D60794A60FE545B
SHA1:	72B34A85DFBFF7C4AEDD8546F2F1AEF2F45C6BD6
SHA-256:	8A660691D65DB7B1D25337F659D8F23996FF2CC0593CD97AE93E43A79394A151
SHA-512:	23360DFBD57C048342C61B87AAD7990420C6209C1BF66A903707E6D64CA889BD9B69110F265373EAA4FC26665B1F82B90958C4B6D19BC3389F80636CEB70C515
Malicious:	false
Preview:	..(4.....Su..C.0.&..0.'..t..s.. p]L..s..<.mK...f5..&;.f......1k.!.....'.r;..y..X#...@.1......D..N..zR..F..#. .J(...L}....J......0.$#e5..Fx.|q...;H..b.^Y......s#....X..V.....N.e..J...../9w1....INLH....f... "...R..8..L......V..h.b./.b.kC9..v@....j.......m.......a#p.L.....*...U.b$...D...{...;..AJ..2....*..%.L.K..r....^.lh...5.........Vz.Y..VIL.$:.8c...........@^Z|=.1T........s<....dQ.[N.LMPv......&. 8m..3;i..|......./R.k+...g.j.L..H....'...Z.Y3.:.86..Z?L.'..H.YS.....1..5>B.P....2.H....{..U`<.,.... .#.&...#..E.%....iAw.}n%T|.j .d.9..3...Y.v3.\......(.s.........#.Ut.s.G*E....b...;.Jh....r3.......= Ar..}.G..K.Y..4S...M.J6P..O].....V.#B{..n..k.Q.....,...,C..5.....s.+.ng...}..SM1b...]!.^.p.nc...l..l......$.C...A."{oSn-..8....am.^.......=|V.T3G..j....v+.-.../..'.....'....RJ..a.W.=#........w.i5H. .^....L....$...H...:....M.x.=.(.....l...Y...Wu....n.&Ai..W.....NL....-.8M.L....T..|.....M.~...am.....$j.U..JUX..@AX.O.....C.`

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.16411908069709
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	ab.exe
File size:	794112
MD5:	0b486fe0503524cfe4726a4022fa6a68
SHA1:	297dea71d489768ce45d23b0f8a45424b469ab00

General

SHA256:	1228d0f04f0ba82569fc1c0609f9fd6c377a91b9ea44c1e7f9f84b2b90552da2
SHA512:	f4273ca5cc3a9360af67f4b4ee0bf067cf218c5dc8caeafbfa1b809715effe742f2e1f54e4fe9ec8d4b8e3ae697d57f91c2b49bdf203648508d75d4a76f53619
SSDEEP:	24576:TCs99+OXLpMePfl8TgmBTCDqEbOpPtpFhyxfq:5GOXLpMePfzVTCD7gPtLhSfq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.I.}.'}}.'}}.'}i.$|I.'}i."|..'}i.#|j.'}i.!|..'}..#|I.'}..$|k.'}.."|..'}i.&|j.'}}.&}..'}...|I.'}...}|.'}}..}|.'}..%||.'}Rich}.'

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x43f186
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:	0x60689947 [Sat Apr 3 16:35:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	b56503b8c4f46a3a086734c09c6bd0f3

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8284c	0x82a00	False	0.488630756579	data	6.60983970569	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x84000	0x2f3d6	0x2f400	False	0.264529596561	data	3.62244340935	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xb4000	0x7818	0x6800	False	0.106745793269	data	3.31661959005	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x5d8	0x600	False	0.453125	data	4.07117757835	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbd000	0x8d44	0x8e00	False	0.518926056338	data	6.64901147486	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ab.exe PID: 6212 Parent PID: 2008

General

Start time:	16:47:33
Start date:	06/01/2022
Path:	C:\Users\user\Desktop\ab.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ab.exe"
Imagebase:	0x10e0000
File size:	794112 bytes
MD5 hash:	0B486FE0503524CFE4726A4022FA6A68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.317257973.00000000043E8000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.316985824.00000000043E8000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_PersistenceViaHiddenTask, Description: Yara detected PersistenceViaHiddenTask, Source: 00000000.00000003.324241984.00000000007E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.324241984.00000000007E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_PersistenceViaHiddenTask, Description: Yara detected PersistenceViaHiddenTask, Source: 00000000.00000003.315481275.00000000007E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.315481275.00000000007E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.321019974.0000000004DB7000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_PersistenceViaHiddenTask, Description: Yara detected PersistenceViaHiddenTask, Source: 00000000.00000003.349826144.00000000007E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.349826144.00000000007E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_PersistenceViaHiddenTask, Description: Yara detected PersistenceViaHiddenTask, Source: 00000000.00000003.354766251.00000000007E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.354766251.00000000007E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.321639243.0000000004DB7000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.321666234.0000000004DB7000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.316551039.00000000043E8000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.317170385.00000000043E8000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.321142835.0000000004DB7000.00000004.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.336845609.000000000083D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000000.00000003.324338080.000000000083D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Key Value Modified

Analysis Process: ab.exe PID: 4876 Parent PID: 664

General

Start time:	16:47:34
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe
Imagebase:	0x12f0000
File size:	794112 bytes
MD5 hash:	0B486FE0503524CFE4726A4022FA6A68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000002.00000002.309597830.000000000069A000.00000004.00000020.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 88%, Virustotal, Browse • Detection: 66%, Metadefender, Browse • Detection: 96%, ReversingLabs
Reputation:	low

Analysis Process: WMIC.exe PID: 4520 Parent PID: 3040

General

Start time:	16:47:35
Start date:	06/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic SHADOWCOPY DELETE /nointeractive
Imagebase:	0x7ff6dc4e0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Written

Analysis Process: WMIC.exe PID: 4800 Parent PID: 3040

General

Start time:	16:47:36
Start date:	06/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic SHADOWCOPY DELETE /nointeractive
Imagebase:	0x7ff6dc4e0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 5876 Parent PID: 4520

General

Start time:	16:47:36
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WMIC.exe PID: 3148 Parent PID: 3040

General

Start time:	16:47:36
Start date:	06/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic SHADOWCOPY DELETE /nointeractive
Imagebase:	0x7ff6dc4e0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 4768 Parent PID: 4800

General

Start time:	16:47:36
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WMIC.exe PID: 1744 Parent PID: 6212

General

Start time:	16:47:37
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic SHADOWCOPY DELETE /nointeractive
Imagebase:	0x950000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 1756 Parent PID: 3148

General

Start time:	16:47:37
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 7084 Parent PID: 1744

General

Start time:	16:47:37
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Reputation:	high

Analysis Process: vssadmin.exe PID: 5468 Parent PID: 6212

General

Start time:	16:47:38
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\vssadmin.exe
Wow64 process (32bit):	true
Commandline:	vssadmin Delete Shadows /All /Quiet
Imagebase:	0x13b0000
File size:	110592 bytes
MD5 hash:	7E30B94672107D3381A1D175CF18C147
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 7204 Parent PID: 5468

General

Start time:	16:47:39
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WMIC.exe PID: 7444 Parent PID: 6212

General

Start time:	16:47:40
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic SHADOWCOPY DELETE /nointeractive
Imagebase:	0x950000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 7496 Parent PID: 7444

General

Start time:	16:47:41
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vssadmin.exe PID: 7608 Parent PID: 6212

General

Start time:	16:47:42
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\vssadmin.exe
Wow64 process (32bit):	true
Commandline:	vssadmin Delete Shadows /All /Quiet
Imagebase:	0x13b0000
File size:	110592 bytes
MD5 hash:	7E30B94672107D3381A1D175CF18C147
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 7616 Parent PID: 7608

General

Start time:	16:47:42
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 7676 Parent PID: 6212

General

Start time:	16:47:43

Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic SHADOWCOPY DELETE /nointeractive
Imagebase:	0x950000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 7684 Parent PID: 7676

General

Start time:	16:47:44
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: vssadmin.exe PID: 7752 Parent PID: 6212

General

Start time:	16:47:45
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\vssadmin.exe
Wow64 process (32bit):	true
Commandline:	vssadmin Delete Shadows /All /Quiet
Imagebase:	0x13b0000
File size:	110592 bytes
MD5 hash:	7E30B94672107D3381A1D175CF18C147
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7788 Parent PID: 7752

General

Start time:	16:47:46
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000

Copyright Joe Security LLC 2022

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ab.exe PID: 1864 Parent PID: 664

General

Start time:	16:48:34
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\ab.exe
Imagebase:	0x12f0000
File size:	794112 bytes
MD5 hash:	0B486FE0503524CFE4726A4022FA6A68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Avaddon, Description: Yara detected Avaddon Ransomware, Source: 00000023.00000002.438770513.0000000001537000.00000004.00000020.sdmp, Author: Joe Security

Disassembly

Code Analysis

Copyright Joe Security LLC 2022