ID: 511734
Sample Name:
SkB6zJ6H3N.exe
Cookbook: default.jbs
Time: 15:28:09
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

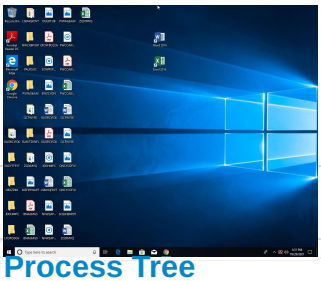
Windows Analysis Report SkB6zJ6H3N.exe

Overview

General Information

Sample Name:	SkB6zJ6H3N.exe
Analysis ID:	511734
MD5:	b8d2d644a3ac5d..
SHA1:	062e29d5960495..
SHA256:	c3f8d6b3e497471.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

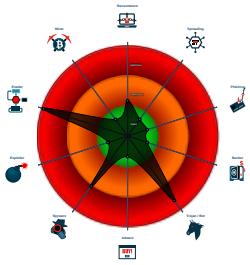
Raccoon
SmokeLoader Vidar

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

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected AntiVM3
- Yara detected Vidar
- Yara detected SmokeLoader
- System process connects to networ...
- Yara detected Raccoon Stealer
- Detected unpacking (changes PE se...
- Antivirus detection for URL or domain
- Found malware configuration
- DLL reload attack detected
- Benign windows process drops PE f...
- Multi AV Scanner detection for doma...

Classification



Process Tree

- **System is w10x64**
- SkB6zJ6H3N.exe (PID: 6372 cmdline: 'C:\Users\user\Desktop\SkB6zJ6H3N.exe' MD5: B8D2D644A3AC5DF8AF9B3AFF803F3347)
  - SkB6zJ6H3N.exe (PID: 6536 cmdline: 'C:\Users\user\Desktop\SkB6zJ6H3N.exe' MD5: B8D2D644A3AC5DF8AF9B3AFF803F3347)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 97A5.exe (PID: 6264 cmdline: C:\Users\user~1\AppData\Local\Temp\97A5.exe MD5: B8D2D644A3AC5DF8AF9B3AFF803F3347)
        - 97A5.exe (PID: 5464 cmdline: C:\Users\user~1\AppData\Local\Temp\97A5.exe MD5: B8D2D644A3AC5DF8AF9B3AFF803F3347)
      - 5D4.exe (PID: 5344 cmdline: C:\Users\user~1\AppData\Local\Temp\5D4.exe MD5: F57B28AEC65D4691202B9524F84CC54A)
        - AdvancedRun.exe (PID: 4288 cmdline: 'C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
          - AdvancedRun.exe (PID: 5596 cmdline: 'C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe' /SpecialRun 4101d8 4288 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
        - powershell.exe (PID: 4756 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user~1\AppData\Local\Temp\5D4.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 4752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - RegSvcs.exe (PID: 6752 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - EDD.exe (PID: 6868 cmdline: C:\Users\user~1\AppData\Local\Temp\EDD.exe MD5: 787AF677D0C317E8062B9705CB64F951)
      - 192F.exe (PID: 3104 cmdline: C:\Users\user~1\AppData\Local\Temp\192F.exe MD5: 73252ACB344040DDC5D9CE78A5D3A4C2)
      - 319A.exe (PID: 4024 cmdline: C:\Users\user~1\AppData\Local\Temp\319A.exe MD5: 9FA070AF1ED2E1F07ED8C9F6EB2BDD29)
        - AdvancedRun.exe (PID: 1432 cmdline: 'C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
      - 69B5.exe (PID: 6140 cmdline: C:\Users\user~1\AppData\Local\Temp\69B5.exe MD5: 539C39A9565CD4B120E5EB121E45C3C2)
      - 32BC.exe (PID: 5540 cmdline: C:\Users\user~1\AppData\Local\Temp\32BC.exe MD5: D02C5BF9533CCE0E9EA3EAFC2F594A49)
- cviueca (PID: 6216 cmdline: C:\Users\user\AppData\Roaming\cviueca MD5: B8D2D644A3AC5DF8AF9B3AFF803F3347)
  - cviueca (PID: 6212 cmdline: C:\Users\user\AppData\Roaming\cviueca MD5: B8D2D644A3AC5DF8AF9B3AFF803F3347)
- cviueca (PID: 6504 cmdline: C:\Users\user\AppData\Roaming\cviueca MD5: B8D2D644A3AC5DF8AF9B3AFF803F3347)
  - cviueca (PID: 2184 cmdline: C:\Users\user\AppData\Roaming\cviueca MD5: B8D2D644A3AC5DF8AF9B3AFF803F3347)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader

```
{
  "C2 list": [
    "http://xacokuo8.top/",
    "http://hajezey1.top/"
  ]
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Vidar_2	Yara detected Vidar	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\EDD.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x43bf:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\319A.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x20735:$x1: https://cdn.discordapp.com/attachments/ • 0x207e9:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\8746.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x4443:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\5D4.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x7b593:$x1: https://cdn.discordapp.com/attachments/ • 0x7b647:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\89D7.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x7ae95:$x1: https://cdn.discordapp.com/attachments/ • 0x7af49:$x1: https://cdn.discordapp.com/attachments/ • 0x7affd:$x1: https://cdn.discordapp.com/attachments/ • 0x7b0b1:$x1: https://cdn.discordapp.com/attachments/

Memory Dumps

Source	Rule	Description	Author	Strings
00000021.00000002.450724070.00000000047F1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000014.00000002.368853755.00000000004A0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000001A.00000002.404074560.00000000004F0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000007.00000000.294055792.000000000311000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000024.00000003.442845982.00000000048A0000.00000004.00000001.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
26.1.cviueca.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
4.1.SkB6zJ6H3N.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
19.2.97A5.exe.2cb15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
28.0.EDD.exe.810000.1.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x43bf:$x1: https://cdn.discordapp.com/attachments/
21.0.cviueca.400000.6.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 28 entries				

Sigma Overview

System Summary:

- Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments
- Sigma detected: Suspicious Script Execution From Temp Folder
- Sigma detected: Powershell Defender Exclusion
- Sigma detected: Possible Applocker Bypass
- Sigma detected: Non Interactive PowerShell
- Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Yara detected Raccoon Stealer
- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected SmokeLoader

E-Banking Fraud:

Yara detected Raccoon Stealer

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

DLL reload attack detected

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Checks if the current machine is a virtual machine (disk enumeration)

Renames NTDLL to bypass HIPS

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected Vidar

Yara detected SmokeLoader

Yara detected Raccoon Stealer

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

Yara detected Vidar

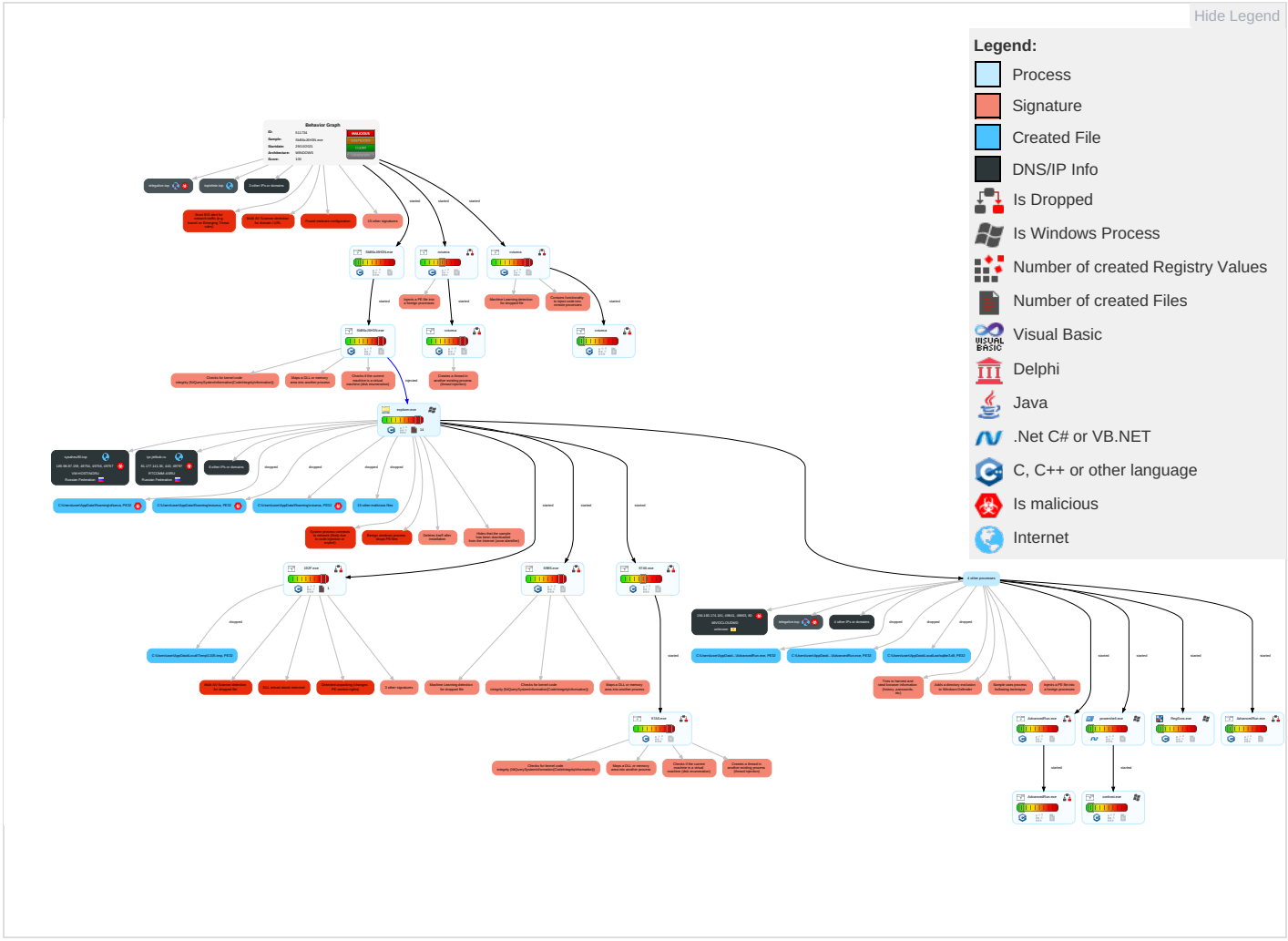
Yara detected SmokeLoader

Yara detected Raccoon Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma Contro
Valid Accounts	Native API 1	DLL Side-Loading 1 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Shared Modules 1	Application Shimming 1	DLL Side-Loading 1 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	Exploitation for Client Execution 1	Windows Service 1	Application Shimming 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 5	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Sta Port 1
Local Accounts	Command and Scripting Interpreter 1 2	Logon Script (Mac)	Access Token Manipulation 1	Software Packing 2 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Ap Layer P
Cloud Accounts	Service Execution 2	Network Logon Script	Windows Service 1	Timestomp 1	LSA Secrets	Security Software Discovery 4 3 1	SSH	Keylogging	Data Transfer Size Limits	Applica Protoco
Replication Through Removable Media	Launchd	Rc.common	Process Injection 6 1 2	DLL Side-Loading 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1 3 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoco
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 6 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

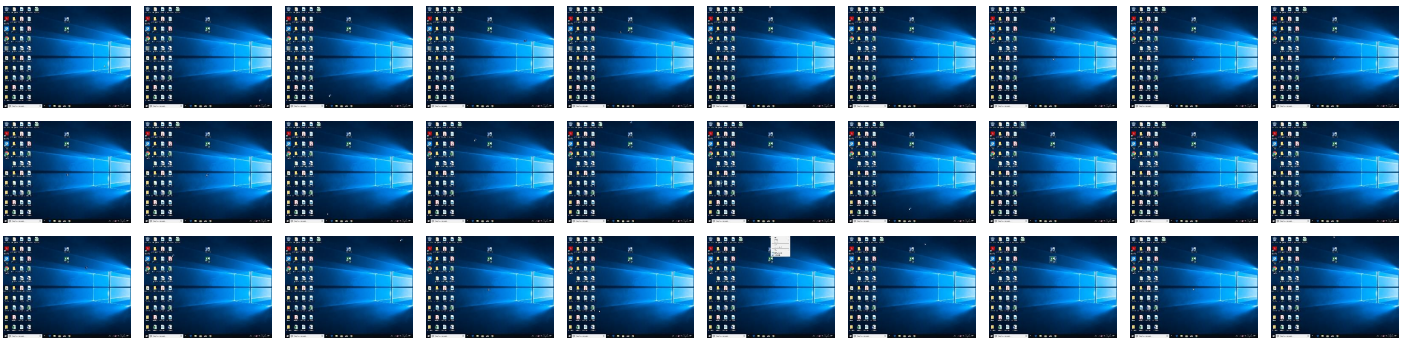
Behavior Graph



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
SkB6zJ6H3N.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\EDD.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5D4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6DDE.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7428.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\69B5.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\cviueca	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\32BC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8746.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\75B0.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\97A5.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\319A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\89D7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\eviueca	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sfiueca	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8E8B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\192F.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1105.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1105.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\192F.exe	80%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\319A.exe	43%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	
C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6DDE.exe	30%	ReversingLabs	Win32.Trojan.Raccrypt	
C:\Users\user\AppData\Local\Temp\75B0.exe	55%	ReversingLabs	Win32.Trojan.Fragtor	
C:\Users\user\AppData\Local\Temp\86B8.exe	14%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
C:\Users\user\AppData\Local\Temp\8746.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.1.SkB6zJ6H3N.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.1.cviueca.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.97A5.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.1.97A5.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.cviueca.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.97A5.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.SkB6zJ6H3N.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.cviueca.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
29.1.192F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.cviueca.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
33.3.69B5.exe.2c10000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.192F.exe.3180e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.SkB6zJ6H3N.exe.2be15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.cviueca.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.97A5.exe.2cb15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.192F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.cviueca.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.cviueca.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.cviueca.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.cviueca.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.97A5.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.69B5.exe.2c00e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.SkB6zJ6H3N.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.cviueca.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
21.2.cviueca.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.cviueca.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.cviueca.2c715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.cviueca.2d815a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.69B5.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.SkB6zJ6H3N.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.cviueca.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
20.0.97A5.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.SkB6zJ6H3N.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.1.cviueca.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.3.192F.exe.3190000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
privacytoolzforyou-6000.top	5%	Virustotal		Browse
iyc.jelikob.ru	12%	Virustotal		Browse
mas.to	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/DetailsDataSet1.xsd	0%	Avira URL Cloud	safe	
http://sysaheu90.top/game.exe	100%	Avira URL Cloud	malware	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://194.180.174.181//l/f/9Z2CynwB3dP17SpzOnMI/7af57f772c6107cc1c44807ee6e54627588ad2f9	0%	Avira URL Cloud	safe	
http://nusurtal4f.net/	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://194.180.174.181//l/f/9Z2CynwB3dP17SpzOnMI/9f3868956801fb92fa090557a1edc6020dc838a9	0%	Avira URL Cloud	safe	
http://194.180.174.181//l/f/_51AzHwB3dP17SpzL5Xz/3fa38023efb6f7516e4aff23353cd7c666085597	0%	Avira URL Cloud	safe	
http://znpst.top/dl/buildz.exe	100%	Avira URL Cloud	malware	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://privacytoolzforyou-6000.top/downloads/toolspab2.exe	100%	Avira URL Cloud	malware	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://194.180.174.181/	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://194.180.174.181//l/f/_51AzHwB3dP17SpzL5Xz/3c5ef2028f9a45f85119eb6cb39f21b264b252bf	0%	Avira URL Cloud	safe	
http://toptelete.top/agrybirdsgamerept	100%	Avira URL Cloud	malware	
http://193.56.146.214/	0%	Avira URL Cloud	safe	
http://xacokuo8.top/	100%	Avira URL Cloud	malware	
http://hajezey1.top/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
privacytoolzforyou-6000.top	185.98.87.159	true	true	• 5%, Virustotal, Browse	unknown
iyc.jelikob.ru	81.177.141.36	true	true	• 12%, Virustotal, Browse	unknown
toptelete.top	172.67.160.46	true	false		unknown
mas.to	88.99.75.82	true	false	• 7%, Virustotal, Browse	unknown
cdn.discordapp.com	162.159.135.233	true	false		high
api.2ip.ua	77.123.139.190	true	false		high
znpst.top	116.121.62.237	true	true		unknown
nusurtal4f.net	45.141.84.21	true	true		unknown
hajezey1.top	185.98.87.159	true	true		unknown
sysaheu90.top	185.98.87.159	true	true		unknown
telegalive.top	unknown	unknown	true		unknown
xacokuo8.top	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sysaheu90.top/game.exe	true	• Avira URL Cloud: malware	unknown
http://194.180.174.181//l/f/9Z2CynwB3dP17SpzOnMI/7af57f772c6107cc1c44807ee6e54627588ad2f9	true	• Avira URL Cloud: safe	unknown
http://nusurtal4f.net/	false	• Avira URL Cloud: safe	unknown
http://194.180.174.181//l/f/9Z2CynwB3dP17SpzOnMI/9f3868956801fb92fa090557a1edc6020dc838a9	true	• Avira URL Cloud: safe	unknown
http://194.180.174.181//l/f/_51AzHwB3dP17SpzL5Xz/3fa38023efb6f7516e4aff23353cd7c666085597	true	• Avira URL Cloud: safe	unknown
http://znpst.top/dl/buildz.exe	true	• Avira URL Cloud: malware	unknown
http://privacytoolzforyou-6000.top/downloads/toolspab2.exe	true	• Avira URL Cloud: malware	unknown
http://194.180.174.181/	true	• Avira URL Cloud: safe	unknown
http://194.180.174.181//l/f/_51AzHwB3dP17SpzL5Xz/3c5ef2028f9a45f85119eb6cb39f21b264b252bf	true	• Avira URL Cloud: safe	unknown
http://toptelete.top/agrybirdsgamerept	true	• Avira URL Cloud: malware	unknown
http://193.56.146.214/	false	• Avira URL Cloud: safe	unknown
http://xacokuo8.top/	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://hajezey1.top/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
81.177.141.36	iyc.jelikob.ru	Russian Federation		8342	RTCOMM-ASRU	true
193.56.146.214	unknown	unknown		10753	LVLT-10753US	false
116.121.62.237	znpst.top	Korea Republic of		9578	CJNET-ASCheiljedangCoIncKR	true
172.67.160.46	toptelete.top	United States		13335	CLOUDFLARENETUS	false
194.180.174.181	unknown	unknown		39798	MIVOCLOUDMD	true
216.128.137.31	unknown	United States		20473	AS-CHOOPAUS	true
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
93.115.20.139	unknown	Romania		202448	MVPShttpswwwmvpsnetEU	false
162.159.133.233	unknown	United States		13335	CLOUDFLARENETUS	false
185.98.87.159	privacytoolzforyou-6000.top	Russian Federation		205840	VM-HOSTINGRU	true
45.141.84.21	nusurtal4f.net	Russian Federation		206728	MEDIALAND-ASRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	511734
Start date:	29.10.2021
Start time:	15:28:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SkB6zJ6H3N.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:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@40/37@64/12
EGA Information:	Failed
HDC Information:	• Successful, ratio: 49.3% (good quality ratio 32.3%) • Quality average: 41.5% • Quality standard deviation: 37.3%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:29:51	Task Scheduler	Run new task: Firefox Default Browser Agent 71E5B89E27185EFF path: C:\Users\user\AppData\Roaming\cvi ueca
15:30:41	API Interceptor	7x Sleep call for process: 32BC.exe modified
15:30:42	API Interceptor	40x Sleep call for process: powershell.exe modified
15:31:03	Task Scheduler	Run new task: Firefox Default Browser Agent FCA2534EFF53B25C path: C:\Users\user\AppData\Roaming\sfi ueca
15:31:07	Task Scheduler	Run new task: Firefox Default Browser Agent 14D0FD35AB9411B6 path: C:\Users\user\AppData\Roaming\evi ueca
15:31:42	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\45135 c8c-e794-4096-a63b-63751937bee2\6DDE.exe" --AutoStart
15:31:57	Task Scheduler	Run new task: Time Trigger Task path: C:\Users\user\AppData\Local\45135c8c-e794-4096-a63b-63751937be e2\6DDE.exe s>--Task
15:32:00	Task Scheduler	Run new task: Telemetry Logging path: C:\Users\user\AppData\Roaming\Microsoft\TelemetryServices\fodh elper.exe
15:32:01	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\451 35c8c-e794-4096-a63b-63751937bee2\6DDE.exe" --AutoStart

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
81.177.141.36	RE0jBlQylG.exe	Get hash	malicious	Browse	• k4dt.jelikob.ru/1780464471.exe
	9d185a3e5184065f1628af9d8325e53b8503a0f7705e5.exe	Get hash	malicious	Browse	• k4d5y.jelikob.ru/854179346.exe
	sboPQqfpHN.exe	Get hash	malicious	Browse	• hwg.jelikob.ru/126808361.exe
193.56.146.214	yj2Lz2zdxp.exe	Get hash	malicious	Browse	• 193.56.146.214/
	HScFcN13Wz.exe	Get hash	malicious	Browse	• 193.56.146.214/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
iyc.jelikob.ru	Md0q201V1D.exe	Get hash	malicious	Browse	• 81.177.141.36
	yj2Lz2zdxp.exe	Get hash	malicious	Browse	• 81.177.141.36
	y1JBw0eea5.exe	Get hash	malicious	Browse	• 81.177.141.36
	21sSRmeUyz.exe	Get hash	malicious	Browse	• 81.177.141.36
	Bi6Q4LEA04.exe	Get hash	malicious	Browse	• 81.177.141.36
	Fo69229D6C.exe	Get hash	malicious	Browse	• 81.177.141.36
	plf5v18Xds.exe	Get hash	malicious	Browse	• 81.177.141.36
	ir7Dw3fZ29.exe	Get hash	malicious	Browse	• 81.177.141.36
	pSY2vVxk86.exe	Get hash	malicious	Browse	• 81.177.141.36
	HScFcN13Wz.exe	Get hash	malicious	Browse	• 81.177.141.36
	w1voKmCYOz.exe	Get hash	malicious	Browse	• 81.177.141.36
	bg5hiAKH5y.exe	Get hash	malicious	Browse	• 81.177.141.36
	e4eukUb6d1.exe	Get hash	malicious	Browse	• 81.177.141.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KZrl2MY8C5.exe	Get hash	malicious	Browse	• 81.177.141.36
	AY5uCs0HrY.exe	Get hash	malicious	Browse	• 81.177.141.36
	Hgny9xwmj6.exe	Get hash	malicious	Browse	• 81.177.141.36
	Pv9fSenm0V.exe	Get hash	malicious	Browse	• 81.177.141.36
	t63ouMqJ8f.exe	Get hash	malicious	Browse	• 81.177.141.36
	pq9FtcL817.exe	Get hash	malicious	Browse	• 81.177.141.36
	gnykCySWj5.exe	Get hash	malicious	Browse	• 81.177.141.36
privacytoolzforyou-6000.top	AyAj5GJqIg.exe	Get hash	malicious	Browse	• 5.188.88.203
	Md0q201V1D.exe	Get hash	malicious	Browse	• 5.188.88.203
	yj2Lz2zdxp.exe	Get hash	malicious	Browse	• 5.188.88.203
	y1JBw0eea5.exe	Get hash	malicious	Browse	• 5.188.88.203
	21sSRmeUyz.exe	Get hash	malicious	Browse	• 5.188.88.203
	Bi6Q4LEA04.exe	Get hash	malicious	Browse	• 5.188.88.203
	rouraiQ4P3.exe	Get hash	malicious	Browse	• 185.185.69.21
	Fo69229D6C.exe	Get hash	malicious	Browse	• 185.185.69.21
	plf5v18Xds.exe	Get hash	malicious	Browse	• 185.185.69.21
	ir7Dw3fZ29.exe	Get hash	malicious	Browse	• 185.185.69.21
	pSY2vVxk86.exe	Get hash	malicious	Browse	• 185.185.69.21
	HScFcN13Wz.exe	Get hash	malicious	Browse	• 185.185.69.21
	w1voKmCYOz.exe	Get hash	malicious	Browse	• 185.185.69.21
	bg5hiAKH5y.exe	Get hash	malicious	Browse	• 185.185.69.21
	e4eukUb6d1.exe	Get hash	malicious	Browse	• 185.185.69.21
	KZrl2MY8C5.exe	Get hash	malicious	Browse	• 185.185.69.21
	AY5uCs0HrY.exe	Get hash	malicious	Browse	• 185.185.69.21
	Hgny9xwmj6.exe	Get hash	malicious	Browse	• 185.185.69.21
	Pv9fSenm0V.exe	Get hash	malicious	Browse	• 185.185.69.21
	t63ouMqJ8f.exe	Get hash	malicious	Browse	• 185.185.69.21

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LVLT-10753US	yj2Lz2zdxp.exe	Get hash	malicious	Browse	• 193.56.146.214
	y1JBw0eea5.exe	Get hash	malicious	Browse	• 193.56.146.214
	Bi6Q4LEA04.exe	Get hash	malicious	Browse	• 193.56.146.214
	vEBWe85OY5	Get hash	malicious	Browse	• 208.51.98.34
	Fo69229D6C.exe	Get hash	malicious	Browse	• 193.56.146.214
	HScFcN13Wz.exe	Get hash	malicious	Browse	• 193.56.146.214
	AY5uCs0HrY.exe	Get hash	malicious	Browse	• 193.56.146.214
	t63ouMqJ8f.exe	Get hash	malicious	Browse	• 193.56.146.214
	wRmHCEnowl	Get hash	malicious	Browse	• 94.154.174.104
	elmb49ofup	Get hash	malicious	Browse	• 94.154.174.115
	f5a160643d5d68888ca63351aa503284c14971b9d6d22.exe	Get hash	malicious	Browse	• 193.56.146.64
	hNsTaM2BAu	Get hash	malicious	Browse	• 168.215.14.42
	eBQ4XSarFt	Get hash	malicious	Browse	• 147.207.217.91
	6Uh6CSZ8oN	Get hash	malicious	Browse	• 147.207.27.141
	Tsunami.x86	Get hash	malicious	Browse	• 94.154.174.132
	nfmAUVANYA	Get hash	malicious	Browse	• 200.24.17.224
	DqvtaJLisV.exe	Get hash	malicious	Browse	• 193.56.146.60
	w347KbpZ6t.exe	Get hash	malicious	Browse	• 193.56.146.60
	V5cy4riN4O.exe	Get hash	malicious	Browse	• 193.56.146.60
	Hm7d40tE44.exe	Get hash	malicious	Browse	• 193.56.146.188
RTCOMM-ASRU	Md0q201V1D.exe	Get hash	malicious	Browse	• 81.177.141.36
	yj2Lz2zdxp.exe	Get hash	malicious	Browse	• 81.177.141.36
	y1JBw0eea5.exe	Get hash	malicious	Browse	• 81.177.141.36
	21sSRmeUyz.exe	Get hash	malicious	Browse	• 81.177.141.36
	Bi6Q4LEA04.exe	Get hash	malicious	Browse	• 81.177.141.36
	Fo69229D6C.exe	Get hash	malicious	Browse	• 81.177.141.36
	plf5v18Xds.exe	Get hash	malicious	Browse	• 81.177.141.36
	ir7Dw3fZ29.exe	Get hash	malicious	Browse	• 81.177.141.36
	pSY2vVxk86.exe	Get hash	malicious	Browse	• 81.177.141.36
	HScFcN13Wz.exe	Get hash	malicious	Browse	• 81.177.141.36
	w1voKmCYOz.exe	Get hash	malicious	Browse	• 81.177.141.36
	bg5hiAKH5y.exe	Get hash	malicious	Browse	• 81.177.141.36
	e4eukUb6d1.exe	Get hash	malicious	Browse	• 81.177.141.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KZrl2MY8C5.exe	Get hash	malicious	Browse	• 81.177.141.36
	AY5uCs0HrY.exe	Get hash	malicious	Browse	• 81.177.141.36
	Hgny9xwmj6.exe	Get hash	malicious	Browse	• 81.177.141.36
	Pv9fSenm0V.exe	Get hash	malicious	Browse	• 81.177.141.36
	t63ouMqJ8f.exe	Get hash	malicious	Browse	• 81.177.141.36
	pq9FtcL817.exe	Get hash	malicious	Browse	• 81.177.141.36
	gnykCySWj5.exe	Get hash	malicious	Browse	• 81.177.141.36

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	21sSRmeUyz.exe	Get hash	malicious	Browse	• 81.177.141.36
	97HaxOZ8Wu.exe	Get hash	malicious	Browse	• 81.177.141.36
	97HaxOZ8Wu.exe	Get hash	malicious	Browse	• 81.177.141.36
	6810825092 ISF - EMC ___ - Draft.scr.exe	Get hash	malicious	Browse	• 81.177.141.36
	ir7Dw3fZ29.exe	Get hash	malicious	Browse	• 81.177.141.36
	pSY2vVxk86.exe	Get hash	malicious	Browse	• 81.177.141.36
	HScFcN13Wz.exe	Get hash	malicious	Browse	• 81.177.141.36
	w1voKmCYOz.exe	Get hash	malicious	Browse	• 81.177.141.36
	bg5hiAKH5y.exe	Get hash	malicious	Browse	• 81.177.141.36
	e4eukUb6d1.exe	Get hash	malicious	Browse	• 81.177.141.36
	KZrl2MY8C5.exe	Get hash	malicious	Browse	• 81.177.141.36
	Hgny9xwmj6.exe	Get hash	malicious	Browse	• 81.177.141.36
	Pv9fSenm0V.exe	Get hash	malicious	Browse	• 81.177.141.36
	lO6Gq6TznP.exe	Get hash	malicious	Browse	• 81.177.141.36
	spectrum_internet_service_level_agreement.js	Get hash	malicious	Browse	• 81.177.141.36
	spectrum_internet_service_level_agreement.js	Get hash	malicious	Browse	• 81.177.141.36
	6oi3E5jdTR.exe	Get hash	malicious	Browse	• 81.177.141.36
	Jm3x80kZjO.exe	Get hash	malicious	Browse	• 81.177.141.36
	J4sqj3xhBf.doc	Get hash	malicious	Browse	• 81.177.141.36
	4BxZpwUFPO.exe	Get hash	malicious	Browse	• 81.177.141.36
54328bd36c14bd82ddaa0c04b25ed9ad	QM5qEGS2aT.exe	Get hash	malicious	Browse	• 162.159.135.233
	TEXTIL_0172PDF.exe	Get hash	malicious	Browse	• 162.159.135.233
	PO202102900010 #QUoTE - 115892.exe	Get hash	malicious	Browse	• 162.159.135.233
	21sSRmeUyz.exe	Get hash	malicious	Browse	• 162.159.135.233
	090-087654123456700890097 65.exe	Get hash	malicious	Browse	• 162.159.135.233
	PO# 5100299028__0001.exe	Get hash	malicious	Browse	• 162.159.135.233
	PAYMENT TRANSFER.exe	Get hash	malicious	Browse	• 162.159.135.233
	- 2021..exe	Get hash	malicious	Browse	• 162.159.135.233
	PeSTW7v5yC.exe	Get hash	malicious	Browse	• 162.159.135.233
	ir7Dw3fZ29.exe	Get hash	malicious	Browse	• 162.159.135.233
	pSY2vVxk86.exe	Get hash	malicious	Browse	• 162.159.135.233
	HScFcN13Wz.exe	Get hash	malicious	Browse	• 162.159.135.233
	w1voKmCYOz.exe	Get hash	malicious	Browse	• 162.159.135.233
	PO10976 B86b0mDlYqpH2306105pdf.doc	Get hash	malicious	Browse	• 162.159.135.233
	bg5hiAKH5y.exe	Get hash	malicious	Browse	• 162.159.135.233
	e4eukUb6d1.exe	Get hash	malicious	Browse	• 162.159.135.233
	KZrl2MY8C5.exe	Get hash	malicious	Browse	• 162.159.135.233
	DHL-SHIPMENT_INFO.exe	Get hash	malicious	Browse	• 162.159.135.233
	qOwryRbbIy.exe	Get hash	malicious	Browse	• 162.159.135.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	987654GYYHGFD34567890-0987TGH.exe	Get hash	malicious	Browse	• 162.159.135.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\AppData\Local\Temp\32BC.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\2U0MzuqSVXm.zip	
Process:	C:\Users\user\AppData\Local\Temp\32BC.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1183
Entropy (8bit):	7.495262700309787
Encrypted:	false
SSDEEP:	24:9ij0WFTWzD9k/UeLp6WUwl5QP8HYE2xt/Qt7me7+F/l:9SoH9k8eLIW5Q62xJQpmkAt
MD5:	B42CE9AAF8B16C05F41321E37F95ABD0
SHA1:	789EC1723324AA43F373304B136136941D46D4D4
SHA-256:	0CF2C9A321BCEF3C946C88435F36CBB5CB80DE9311E133B8853884FE6A30586D
SHA-512:	CC23DA73DBE44608D0D97B6F840FD70AEFF651162596E828D04B31172960D592A616E2D577B70B4DEA091216BA425790F27FADC62532E80745A0959C41D515D4
Malicious:	false
Reputation:	unknown
Preview:	PK.....F|]SXVQ.....*...browsers/cookies/Google Chrome_Default.txtUT.....|a..|a..|a%..n. ...K.)t....#H..\U ..6.(.k...w.....v.....Y....a..0L..`$@a.f.yp....^.G. j..ur.J.n.DD.e slF.;s.Vz..;..0.S%R...L~.3)..v.m...P..._.;..s...\$...F@w...\.h....."..3>.1.[.%.....%.w.%f.....PK.....\|]Si.I....E.....System Info.txtUT.....\|a..\|a..\|auSMo.0.=.J..s$RA...8-.j..t.$.J.T...U b#.....;4.m..".y..<.ff-.....I..s.....UU..9..P.Ff.m%.....X..qFc`.Q._.V.{Y.h.7,.$`)..X.FY...r..N.4....f$....q...h..~....4]...O.....=..u...;...tXc...s.....J8.dl.....5.....h..Y..#.B.Z.C7 .zW).....1..~.{....*.$..8.,.x.^....D. ..SH.>.)!...b....yR....%x..I.^.n.i..._N8g..k'.~.?:.E.(].'....$...M.\|YYS.....LI..\...>..8..Y]g.`#+o=.....p.c....._..p.tC%.\|...r...<.....VJ.x.T..=...L....)WW..G.Q..\....,Ua.3..L.S.;-/E..}9I....p...Q.....I.Q.N4.....fS.h....FH.....9HI..H..$.(....u.dp....<..A.qV....Q@2.....Bx (.....Y(...t`..q.a..R.O..)-...u.~M.(.X.. d.D50/Ug....PK....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\AppData\Local\Temp\32BC.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\Tx3inWO7Su	
Process:	C:\Users\user\AppData\Local\Temp\32BC.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4588965670203364
Encrypted:	false
SSDEEP:	48:T1YBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:OWU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	16C3DE08951964D7D40D5205692A3D82
SHA1:	EA06159A8A50E853806DD09F830B0C39E3374E75
SHA-256:	2DB39320E9691AC1690723A33BC7AA2330B1B63621B3AFAEDBEB0E10463192F5
SHA-512:	E0B54313A7A6188DC711CCDC7854CEF3456D79BA1E29AF7BD7310733B03167434D063C3D51DBB63D426919088104D46CA42815DEF9337B4C604F1DD0150CCE5
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\AppData\Local\Temp\32BC.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\AppData\Local\Temp\32BC.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\32BC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... .....".....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsr c..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\319A.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\319A.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7K84jE4Ks:MxHKXwYHKhQnoPtHoxHhAHKzvKvjHKs
MD5:	AE8CFF33270358D6EC23793128B3EF2F
SHA1:	5E6B156157EDEA4222A5E0C258AE9ADEBB8CB7CE
SHA-256:	498EAB9F855E7CE9B812EAD41339A9475127F0C8E7249033B975071D2292220C
SHA-512:	473111AD332D5E66724AFB0CE5A1E1C97890D60484A818D1DB8C2386A99C05BAE6C9D5C535DDFB6790BF5707C153502B938BE201393A3D70342A62902E0A3C9
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5D4.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\5D4.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7K84jE4Ks:MxHKXwYHKhQnoPtHoxHhAHKzvKvjHKs
MD5:	AE8CFF33270358D6EC23793128B3EF2F
SHA1:	5E6B156157EDEA4222A5E0C258AE9ADEBB8CB7CE
SHA-256:	498EAB9F855E7CE9B812EAD41339A9475127F0C8E7249033B975071D2292220C
SHA-512:	473111AD332D5E66724AFB0CE5A1E1C97890D60484A818D1DB8C2386A99C05BAE6C9D5C535DDFB6790BF5707C153502B938BE201393A3D70342A62902E0A3C9
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22168
Entropy (8bit):	5.605445164688419
Encrypted:	false
SSDEEP:	384:etCDLqoZI5K1rpl9z6vOMSBKnAjultI+P7Y9gtSJ3xeT1MaXZlgRV7+3HmZBDI+s:+6rP904KAClthrtc8C+fYLVi
MD5:	68AE69A585A398F9AFA7BD9FCC17E62F
SHA1:	C5164B582D9A3C6020D0717694906CFB80BCD648
SHA-256:	4BC8D9F5E97175B8377C5FC31965D691A255A516EB3EF56ED9540B41C4258F06
SHA-512:	941F79F18F10DAE389D27E6CFB2FD12C4836A7E82F1A788BF5562A98E029531DABAE6B285A9A7ADA4AA25FDEC661D3BB2193B70CB2636D7239D35C1F372AA4E1
Malicious:	false
Reputation:	unknown
Preview:	@...e.....^.....h.>.).....B...I.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Local\Temp\5D4.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@.....

C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\test.bat	
Process:	C:\Users\user\AppData\Local\Temp\5D4.exe

C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\test.bat	
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\1105.tmp	
Process:	C:\Users\user\AppData\Local\Temp\192F.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	1622408
Entropy (8bit):	6.298350783524153
Encrypted:	false
SSDEEP:	24576:hNZ04UyDzGrVh8xsPCw3/dzcldJndozS35lW1q/kNVSYVEs4j13HLHGJImdV4q:dGrVr3hclvnqzS35lWk/LvRHb0
MD5:	BFA689ECA05147AFD466359DD4A144A3
SHA1:	B3474BE2B836567420F8DC96512AA303F31C8AFC
SHA-256:	B78463B94388FDDB34C03F5DDDD5D542E05CDED6D4E38C6A3588EC2C90F0070B
SHA-512:	8F09781FD585A6DFB8BBC34B9F153B414478B44B28D80A8B0BDC3BED687F3ADAB9E60F08CCEC5D5A3FD916E3091C845F9D96603749490B1F7001430408F711D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L!y>.@.m.@.m.@.m...l.@.mg$.l.@.mg$.lN@.mg$.l.A.mg$.l .@.mg$.l.@.mg$.m.@.mg$.l.@.mRich.@.m.....PE..L...s<s.....!.....P....(K.....@A.....&.....8.....h...Y.. .....N..`l..T.....text....).....*..... ..`RT.....@..... ..`.data...dW...P.....0.....@....mrdata.h#.....$...>..... ....@....00cfg.....b.....@..@.rsrc...8.....d.....@..@.reloc...N.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\192F.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.734269361613487
Encrypted:	false
SSDEEP:	3072:UJ+Dg6a/6BO0fFI4+uX67vtk4nNcDxzyuEpuVMO6P2+BwvHJ3/RA:FDy/6BOSFI48v2dxzyuEpynVP
MD5:	73252ACB344040DDC5D9CE78A5D3A4C2
SHA1:	3A16C3698CCF7940ADFB2B2A9CC8C20B1BA1D015
SHA-256:	B8AC77C37DE98099DCDC5924418D445F4B11ECF326EDD41A2D49ED6EFD2A07EB
SHA-512:	1541E3D7BD163A4C348C6E5C7098C6F3ADD62B1121296CA28934A69AD308C2E51CA6B841359010DA96E71FA42FD6E09F7591448433DC3B01104007808427C3DE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 80%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....^.....V.....,.....p....@.....q.....\...<.... ..8.....q.....@.....p..x..... .....text....U.....V..... ..`.rdata...G...p...H...Z.....@..@.data...DB.....@....cipizi.r.....@..@.rsrc...8.... .....@..@..... ....

C:\Users\user\AppData\Local\Temp\319A.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	161280
Entropy (8bit):	5.163359140538006
Encrypted:	false
SSDEEP:	3072:hj1+ax5s9jVultxyIAMzTjSMzTjoIe1UhCp:hJqjVoeN
MD5:	9FA070AF1ED2E1F07ED8C9F6EB2BDD29
SHA1:	6E1ACD6CB17AB64AC6DBF0F4400C649371B0E3BD
SHA-256:	08D67F957EC38E92301EEAAAF2759EF2A070376239EAD25864C88F3DD31EAB8C
SHA-512:	14A1CD1090A2ECCEA3B654EEE2B7D4DE390219F8C3C200D97D2AB431311BDF24B1B40F2F38E78804AD286654CD33DFB515704C9B863DAF0786A0D633F05C9B2
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\319A.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0.wa.....P..l..... .....@.. .....@.....O.....x..... ....H.....text....k... ...l..... ..`.rsrc.....n.....@..@.reloc.....t.....@..B.....H.....(u..t.....A...HL...(.....M...Z.....@.....!.....L.....!...T...h...i...s... ...p...r...o...g...r...a...m... ...c...a...n...n...o...t... ...b...e... ...r...

C:\Users\user\AppData\Local\Temp\32BC.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	602112
Entropy (8bit):	7.0892638670378805
Encrypted:	false
SSDEEP:	12288:kGukYO+PJKZ0NZviBsCUcU9Yveqgg4Q2K+:HukCJ1iiCf202
MD5:	D02C5BF9533CCE0E9EA3EAFC2F594A49
SHA1:	843BC6B17AD8AF53CE851F5C05D21BC03B434E5C
SHA-256:	32C06152828C3D144B82E6E1F4EF18381BE1DFD307105851827E358C64156949
SHA-512:	A0E6A4157A13891FF91E20860D320E137A6D1D33629371D29598D40E53CFDEED86D2B0D0F8BF668A9B8175623662807DB190360414640BDAD5261B2702D148D5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.m.m.m..2m..m...m..m..3mq..m...m...m.m...m..6m...m...m...m ...m...mRich.m.....PE..L...D,._.....p.....@.....x.....@.....D...d....Pw..<.....w....0..... ....@.....text...x..... ..`.data....io.....@....malajew.....@w.....@....rsrc....<...Pw..<.....@..@.reloc...#.. ..w..$.....@..B.....

C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Local\Temp\319A.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\AdvancedRun.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\test.bat	
Process:	C:\Users\user\AppData\Local\Temp\319A.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\5D4.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	512512
Entropy (8bit):	7.846723941917503
Encrypted:	false
SSDEEP:	12288:Tw86shtDE09VgbshnKMstp7eylszgTDzLTDaMqvK8J+LF:TVhdLVg2Zep7njXzPDxC+J
MD5:	F57B28AEC65D4691202B9524F84CC54A
SHA1:	F546B20EB40E3BC2B6929BA0F574E32422CED30C
SHA-256:	87D86132095541ED3B5FE05EB06692E1712287B6FFD9832A28EB85F52B55F0A5
SHA-512:	1A773186B0A15F743F8D9681036A9ECA45E2DD5F7944725498E929C5438ACFFCD753061EB475383E5759FC41A8ADE4EB717F3D3529313C3C0D48C659B5E36F09
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\5D4.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. .....@..... .`.....S..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... . .....@..B.....H.....u...p.....HZ..X.....MZ.....@.....!....!This program cannot be run in DOS mode....$.....PE.....\" ..P.....Z8... ...@..... .....@.....8..O....@..x.....`.....7..... ... ..... ..H.....text...`.... .....

C:\Users\user\AppData\Local\Temp\69B5.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	348672
Entropy (8bit):	5.997778327285649
Encrypted:	false
SSDEEP:	6144:0BbSn3n6QHUKl3hINRqdhUm6b8mCcNebxCg1:Eu3n6UUKlxS2Um6b8mCcNej
MD5:	539C39A9565CD4B120E5EB121E45C3C2
SHA1:	5E1975A1C8F9B8416D9F5F785882DFB0CC9161DC
SHA-256:	C673B8408DB0EB515651E6A6F3361C713903001011C6E13A1825C0376A83D1DD
SHA-512:	3CC343A53051BE34B4CAD9AA9A9AE68D6B5A978B2ECD10516E4934452D29A9455A6CEB5EB7C7B691B2D08F1781BFB7B1E3627CB2823DD4F60860861F2202BAF
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\69B5.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5.>.T.m.T.m.T.m."2m.T.m.".m.T.m."3mqT.m.,.m.T.m.T.m .T.m."6m.T.m.".m.T.m.".m.T.mRich.T.m.....PE..L....8?`.....v.....`.....@.....z.....f.....$...d....py..l.....y..... .....@.....text..... ..`.data...H.u.....@....rsrc....l...py..J.....@..@.reloc...#....y..$.....@..B..... ....

C:\Users\user\AppData\Local\Temp\6DDE.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	877056
Entropy (8bit):	7.462302194895007
Encrypted:	false
SSDEEP:	24576:yYuSM7Gp8zSjQLCV9ibUqyuziiM95BxXEr:yv7i8zSjbVwB1ZM910r
MD5:	B79D3399603938A695A98A75DCFBAB91
SHA1:	AF9A85F2CC85CD3B040536C988AAB45C237A22D9
SHA-256:	934690E391745FCA58CA0DF6D41952D6F58ED7B18AB8FDDA22484B01EB262BE8
SHA-512:	5499156CB77B33218077A690AF2EC89D9E9C2AC20796BB2F0A889DD97E569DDD84FDEC0F7C9332523A95D47081235E1BD2240D2971CDD5153CFA906C39BFA0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.m.m.m..2m..m...m..m..3mq..m...m...m.m...m..6m...m...m...m ...m...mRich.m.....PE..L.....\_.....p..... .....@.....\|....ja.....d....{..<.....{.....0.....@..... .....text..... ..`.data....io.....@....vuci.....p{.....@....rsrc....<....{..<.....@..@.reloc...#....{..$...>..... ....@..B..... .....

C:\Users\user\AppData\Local\Temp\7428.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604160
Entropy (8bit):	7.081312542094628
Encrypted:	false
SSDEEP:	12288:zUq737aTz5aNquRVgE6/kEObrF5d/WYN4t88+wGOjsyDR:Aq7rwa0uRm8brF5LupDs
MD5:	DE692F1B4D4C63FED395BE25E878858E
SHA1:	16F5B74E898FB0CD30F127CB1E03DA79E481158A
SHA-256:	6ED753E5B9A7AC5D89A6F9749E24C5BEB7483C6FDA2057E81E1EB3ED5A32AB21
SHA-512:	24227BBCD1451E7F6A2B6C16637987B1388BE398A88005851AF24805BFD7B57AE39AE7B70E69DE3B424EE48E4FB65EF0CABD710692EBC9393F2A1542E6D8E06 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5.>.T.m.T.m.T.m."2m.T.m.".m.T.m."3mqT.m.,.m.T.m.T.m .T.m."6m.T.m.".m.T.m.".m.T.mRich.T.m.....PE..L.....*\_.....v.....@.....@.....~.....4.....d....P}..l.....}..... ....@.....text..... ..`.data...H.u.....@....rsrc....l...P}..J.....@..@.reloc...#....}..$.....@..B..... ....

C:\Users\user\AppData\Local\Temp\75B0.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	278528
Entropy (8bit):	7.390894610588505
Encrypted:	false
SSDEEP:	6144:IdQPlt1M8RJNHUMb62VCDuy1DzJDGLkjNVlZeJjuzbgwuA7ITsq:lalt6mJN0x2VmlhtawtcjunnF7
MD5:	FA00DF47BCC5F9AD16ED71856FB6F4D6
SHA1:	561D89B6384A44E6D47AC4B68D04FFFFF3DE3558
SHA-256:	B2F5636B2E78B3F60EA53FD0C7C95656E11C08FAC59869B38A165C7BF39CF1E5
SHA-512:	3A6ACB14B041B341C979F233D881225615B225DAC9E84F0CD62DAEC69818212A9620AE82E4B61BA5547E3A0EB9D1D8442EF52CE86BF093918203D33DDF3283C
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\75B0.exe

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 55%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....`.....6....._%.....@.....(....`..H/.....@.....p..... .....text..... ..`.rdata...E.....F.....@..@.data....<.....@....xoj....r....P.....@..@.rsrc...H/...`...0.....@..@..... ....

C:\Users\user\AppData\Local\Temp\86B8.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	262248
Entropy (8bit):	7.344044114091331
Encrypted:	false
SSDEEP:	6144:7Zd5yNguYYTkxcNQoF8KzJugf/vTvN9KQqJlo:7Zd5yNguPQyNQYJuSvDLKXlo
MD5:	EDE62358EA39643E43992E9068E03CA2
SHA1:	0F73E8F96C01135A91D4E1BFECA139AD31C72C15
SHA-256:	187CB817751D6871EB7BE566DD9D9A98A46EDB11391220B69E4FAD695F31E605
SHA-512:	552B31EDA2131C8326996DEBA1812C6A6B23D892DDABDD17C3182FCD43B9019CFC863EED1FF67FA2EC21297E98F61502D3E095972D2C6710D08B3F27EA821
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 14%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{a.....0..... ... .@.. .....@..... ..@.....(...W.....XH.....h.... ....H.....text..... ....`.rsrc...XH.....J.....@..@.rel oc..... .....@..B.....d.....H.....l...."..... .....?.....?.....?..... .....?..... .....@..... .....@..... .....@..... .....

C:\Users\user\AppData\Local\Temp\8746.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	27576
Entropy (8bit):	5.969933955399239
Encrypted:	false
SSDEEP:	384:bekc2D26R7pXha5eglsu2CfQG9kyf4ZZK61TEYFGc1QzOQs42Aghgn:bJcMnacgl6EWlXzZ1QO4khgn
MD5:	FA6D8115D2266A121FE7C1552C0DDDFD
SHA1:	9166433A1F42AE7A623F26341DD9BBED91A045B3
SHA-256:	237E9E25B4DADE7BD2CCD0F6D59C9D607EEED8E60C1041F10BE3D4C50B37A459
SHA-512:	58825BAF9D243279393A635AEE9E7493682F18105D24CFAAF270BFAE54CB2FFDFE12734D7E3EB34983C554F3599BB73D523029871F28D8AFBF25CD27798C2368
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\8746.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..N.....I... .....@.. .....G... .`.....I..O.....,.....X..... .....H.....text....L... ...N..... ..`.rsrc...,.....P.....@..@.reloc..... .....V.....@..B.....I.....H.....PK..L!.....MZ.....@.....!...!This program cannot be run in DOS mode....$.....PE....." ..P.....Z8... ...@..... .....@.....8..O....@..x.....`.....7..... .. ..H.....text...`.... .....

C:\Users\user\AppData\Local\Temp\89D7.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	510976
Entropy (8bit):	7.850749525333838
Encrypted:	false
SSDEEP:	12288:Iw86shtDE09VgbshnKMstp7eylszgTDzLTDaMqvK8J+W:IVhdLVg2Zep7njXzPDxC+W
MD5:	B0A956B96769AA21A44206DD528C5B39
SHA1:	30CF20E67DFA3FC38C6E80B761AD0D523C5AF43A
SHA-256:	37B78E9A50830B88E97F6048F90EA0AFE925E0C6E4F0E9A1CF3C7849787D9C4C

C:\Users\user\AppData\Local\Temp\89D7.exe

SHA-512:	5B6D8707FA2D4B7D41D7B1733409A34645DF2B42FF064D9E7643A8F4AE7076A798B2012959AF6F8B30E44D60B28EF4B1761E0CB3287448329C9144AE9FD9CE9F
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\89D7.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....N.... .....@.. .....@.....yq... .`.....K..... ..... ..H.....text...T.... ..... ..`.rsrc.....@..@.reloc..... . .....@..B.....0.....H.....u..hk.....@Z..X.....MZ.....@.....!....!This program cannot be run in D OS mode....$.....PE.....' ..P.....Z8... ...@..... .....@.....8..O....@..x.....`.....7..... ... ..... ..H.....text...`.... .....

C:\Users\user\AppData\Local\Temp\8E8B.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	791552
Entropy (8bit):	7.368824467033047
Encrypted:	false
SSDEEP:	12288:uDMkBTpEvda0f6dSctc54lTQazT6A/9Or+ilw8lCW0k7ro8R3D3INLf3:QMk+dV6dS6KazZ4rPlw8lCWYQi
MD5:	7917305400EE899130B1D5B7AFA0A159
SHA1:	D45E1A34FE773040D7034A80BBEBB3DBD3EA4252
SHA-256:	80C4B12305B41D2FDCD9DCCD53D2414C3AEA2188198F3D79AF262709C1E2DAC9
SHA-512:	417DECA0BEEE73B6EA8379B85726A9DAAF4DC32721D7A658BA42B9D359A6739F7478D3E0068C8B110497CB222956A1AFA5E1BF28C202965DEDE7A659EB824EF6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.....^.....Rich..... ...PE..L...m;._.....v.....@.....P....0...I..... .....~..@..... .text..... ..`.data...H.u.....@....rsrc....I...0...J.....@..@.reloc..8$.....&.....@..B..... .....

C:\Users\user\AppData\Local\Temp\97A5.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	345600
Entropy (8bit):	6.002783867482684
Encrypted:	false
SSDEEP:	6144:NOTOeA4lwH4QNlDembw1wCuVB/cChQoyYtCv3ddx/W:NiOePwHjNlDePuVB/cChQoytjx/W
MD5:	B8D2D644A3AC5DF8AF9B3AFF803F3347
SHA1:	062E29D59604956A4CFFD64FC81CD1C3F72B0FF3
SHA-256:	C3F8D6B3E497471CC5E1526D59F7068F0655704F98DCA59D79A77B81F1CB7FD5
SHA-512:	1C3E8F1AD4CC920F2B6815F87C351363E114290811D395790918744452B8ACDF2FDF753AC873CB3FCD115E70FD66DFC59C5A08E38F20080D655FCD88483415A/
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.m.m.m..2m..m...m..m..3mq..m...m...m.m...m..6m...m...m...m ...m...mRich.m.....PE..L.....\_.....p.....p.....@.....t.....4...d....`s..<.....s.....0.....@..... .....text...h..... ..`.data....io.....@....xemu.....Ps.....@....rsrc....<...`s..<.....@..@.reloc...#....s..$..." ....@..B..... .....

C:\Users\user\AppData\Local\Temp\EDD.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	22528
Entropy (8bit):	5.395556088889033
Encrypted:	false
SSDEEP:	384:ezekc2D26R7pXha5eglsu2tiP39n+NDr7vGuywqFGc1QzOQslg:qJcMnacgl6Q10rSuywCZ1QO
MD5:	787AF677D0C317E8062B9705CB64F951
SHA1:	41BF391CE44004A22BA7F18E5FDCDCFCEA73E38F
SHA-256:	7CFA3F3EBB7DCE336E24DF02D5BA0FDBC081927892D597986113FB11EDF1702E

C:\Users\user\AppData\Local\Temp\EDD.exe	
SHA-512:	8A9BF2D0DF12926F3253DCF5F2B5186928107C36189F404C50C69B67BC09DDA267FACD53E3259ABF3934DE6682BC3B0E49D1D5ACCFA5D4A5B702F4F9EF8D8E5
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\EDD.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..N.....nl... .....@.. .....P.... .`.....I..S.....Z..... ..... ..H.....text...tL... ...N..... ..`.rsrc.....P.....@..@.reloc..... .....V.....@..B.....PI.....H.....PK... .....MZ.....@.....!....!This program cannot be run in DOS mode....$.....PE....." ..P.....Z8... ...@..... .....@.....8..O....@..x.....`.....7..... ... ..... ..H.....text...`.... .....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v10ptpcx.iby.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Roaming\beuawud	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	337526
Entropy (8bit):	**7.999338951800792**
Encrypted:	**true**
SSDEEP:	6144:AvGRP66xZSKUZlmY9Y4pck/283ajKg+CvJKoVjPmZMqHc/qrIsiNJ5ixSDJ:AUPBxZCll3pxfqjWC9mY/qrIsiNHRDJ
MD5:	73B48815E85A62D84F5BB46E31D67AA7
SHA1:	74D3CF9931564A828E3D594ECB105FA80A4D596C
SHA-256:	BD35FD2B3538D2966514E2518B63BFD40B35608E49CBC6F7829EF5019D3C650D
SHA-512:	B01FA20CCA894371B79F467070BD11C4B041EB525ED95BC46F52CBFDE16C349DC32C4F6725D11938552400DE9E4A467633D0038AFBB10FE2C0BD75B56B11197
Malicious:	false
Reputation:	unknown
Preview:	.s...v{p}.....C...f....B..$..d..F..k.".P"./.-.....t.....5..vV.~.#.[..w.t...!>u.9..\.o...f^S.Z.iBV.r.c'{TC.....^}=.d.;9....S<U.....T.|.....r...z..a.jK.S..cJ?t....$2.tu7*..B7.4....`...T...vp.7..TD...^. ...O4..&B...9..,....x:.o..z.fR...Q...7..{....3.....oE..l.(.%.6.}.Sx6.....C....x.+l.....~e..@_.8...h.Rvir..S.Z5.-...a.1..l~..f....Nu.fl.{vc..O..'.%M.....|k.cG..D.ix.....35...z'....Z..W.B0.%... (.]#kI)...*...0v...?y.Z8a.x..50.W....?@N.....y.V..].P.&80.....PhZ.sI|'.#6.."...T..X~Jv..4...w.....3.....L.=.o.J`...<i.+O...Xw..?.v.../?.TnR..~P].:.....*.....1\}\..h.E>M.....k <J.gG.y..lX.~.....@...9Q...a.u.....u..Y.w1^G@.....s..s...C.l..P.v`.....^.....H..#y.|.A..K.e...>.#U.,...K7w.^..Z4....:V...p...-;0,J...85.z...$.!.y..h.....SM``{.c...[`..j.....= W.B|.B..xC.>./...P..G..=G....g..f....e.8.z.*.....s..7..ty&Xp1.O..9...N.^hu%{y?....Z...3...".>l..o.e.....l}..S*F..!.....G.r..o.8y.v...!F.D.d....\.T...].9.e09.....

C:\Users\user\AppData\Roaming\cviueca	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	345600
Entropy (8bit):	6.002783867482684
Encrypted:	false
SSDEEP:	6144:NOTOeA4lwH4QNlDembw1wCuVB/cChQoyYtCv3ddx/W:NiOePwHjNlDePuVB/cChQoytjx/W
MD5:	B8D2D644A3AC5DF8AF9B3AFF803F3347
SHA1:	062E29D59604956A4CFFD64FC81CD1C3F72B0FF3
SHA-256:	C3F8D6B3E497471CC5E1526D59F7068F0655704F98DCA59D79A77B81F1CB7FD5
SHA-512:	1C3E8F1AD4CC920F2B6815F87C351363E114290811D395790918744452B8ACDF2FDF753AC873CB3FCD115E70FD66DFC59C5A08E38F20080D655FCD88483415A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Roaming\cviueca	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.m.m.m..2m..m...m..m..3mq..m...m...m.m...m..6m...m...m...m ...m...mRich.m.....PE..L....._.....p.....p.....@.....t.....4...d....`s..<.....s.....0.....@..... .....text...h..... ..`.data....io.....@....xemu.....Ps.....@....rsrc....<...`s..<.....@..@.reloc...#....s..$...".....

C:\Users\user\AppData\Roaming\cviueca:Zone.Identifier	
Process:	C:\Windows\explorer.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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\eviueca	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	348672
Entropy (8bit):	5.997778327285649
Encrypted:	false
SSDEEP:	6144:0BbSn3n6QHUKl3hINRqdhUm6b8mCcNebxCg1:Eu3n6UUKlxS2Um6b8mCcNej
MD5:	539C39A9565CD4B120E5EB121E45C3C2
SHA1:	5E1975A1C8F9B8416D9F5F785882DFB0CC9161DC
SHA-256:	C673B8408DB0EB515651E6A6F3361C713903001011C6E13A1825C0376A83D1DD
SHA-512:	3CC343A53051BE34B4CAD9AA9A9AE68D6B5A978B2ECD10516E4934452D29A9455A6CEB5EB7C7B691B2D08F1781BFB7B1E3627CB2823DD4F60860861F2202BA F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5.>.T.m.T.m.T.m."2m.T.m.".m.T.m."3mqT.m.,.m.T.m.T.m .T.m."6m.T.m.".m.T.m.".m.T.mRich.T.m.....PE..L....8?`.....v.....`.....@.....z.....f.....$...d....py..l.....y..... ....@.....text..... ..`.data...H.u.....@....rsrc....l...py..J.....@..@.reloc...#....y..$.....@..B.....

C:\Users\user\AppData\Roaming\sfiueca	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.734269361613487
Encrypted:	false
SSDEEP:	3072:UJ+Dg6a/6BO0fFI4+uX67vtk4nNcDxzyuEpuVMO6P2+BwvHJ3/RA:FDy/6BOSFI48v2dxzyuEpynVP
MD5:	73252ACB344040DDC5D9CE78A5D3A4C2
SHA1:	3A16C3698CCF7940ADFB2B2A9CC8C20B1BA1D015
SHA-256:	B8AC77C37DE98099DCDC5924418D445F4B11ECF326EDD41A2D49ED6EFD2A07EB
SHA-512:	1541E3D7BD163A4C348C6E5C7098C6F3ADD62B1121296CA28934A69AD308C2E51CA6B841359010DA96E71FA42FD6E09F7591448433DC3B01104007808427C3DE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....^.....V.....,.....p....@.....q.....\...<.... ..8.....q.....@.....p..x..... .....text....U.....V..... ..`.rdata...G...p...H...Z.....@..@.data...DB.....@....cipizi.r.....@..@.rsrc...8.... .....@..@.....

C:\Users\user\Documents\20211029\PowerShell_transcript.855271.tma_ZGFX.20211029153038.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5837
Entropy (8bit):	5.405294114196077
Encrypted:	false
SSDEEP:	96:BZjK6CNMqDo1Zt5Zjt6CNMqDo1Zt6UWMjZj46CNMqDo1Ztmx88T+ZJn:Prni9B2Yn
MD5:	18D3931C59BBA4D325E29740961DC7FF
SHA1:	18AAA967A257D78A55234DB1CBFD9302882A50A6
SHA-256:	B33CEA91BE89E9DE0F9AD6E9BAC53E334D5DB1CFBD4ADB72B5E4F16ACD204BE2
SHA-512:	E8F520B2C1148FC8044192D7C60A2E1A6E364673B3C6EF4FD3E20EA9CCE081D31787BC11A0941238FBA7F6BBFA41E4CAD763D23E23CE057F23562A0AD86349FD
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211029153041..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 855271 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user~1\AppData\Local\Temp\5D4.exe -Force..Process ID: 4756..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211029153041..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user~1\AppData\Local\Temp\5D4.exe -Force..**********..Windows PowerShell transcript start..Start time: 20211029153543..Username: computer\user..RunAs Us

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.002783867482684
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:	SkB6zJ6H3N.exe
File size:	345600
MD5:	b8d2d644a3ac5df8af9b3aff803f3347
SHA1:	062e29d59604956a4cffd64fc81cd1c3f72b0ff3
SHA256:	c3f8d6b3e497471cc5e1526d59f7068f0655704f98dca59d79a77b81f1cb7fd5
SHA512:	1c3e8f1ad4cc920f2b6815f87c351363e114290811d395790918744452b8acdf2fdf753ac873cb3fcd115e70fd66dfc59c5a08e38f20080d655fcd88483415aa
SSDEEP:	6144:NOTOeA4lwH4QNlDembw1wCuVB/cChQoyYtCv3ddx/W:NiOePwHjNlDePuVB/cChQoytjx/W
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>...m...m...m..2m...m...m...m..3mq..m...m...m...m...m..6m...m...m...m...m...mRich...m.....PE..L....._.....

File Icon

Icon Hash:	aecaae9ecea62aa2

Static PE Info

General

Entrypoint:	0x41c770
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F030C83 [Mon Jul 6 11:35:31 2020 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	e522cb867082e04c7a4b61561f8516ce

Entrypoint Preview

Rich Headers

Data Directories

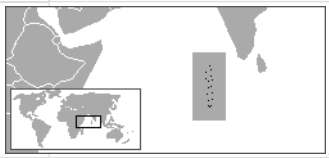
Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3c768	0x3c800	False	0.59776520532	data	6.98541058643	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x3e000	0x26f69c8	0x1600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.xemu	0x2735000	0x2e5	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2736000	0x3c00	0x3c00	False	0.746549479167	data	6.42298314809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x273a000	0x123f0	0x12400	False	0.0814158818493	data	1.05267442442	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Spanish	Paraguay	
Divehi; Dhivehi; Maldivian	Maldives	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 15:29:50.174997091 CEST	192.168.2.7	8.8.8.8	0xe98a	Standard query (0)	xacokuo8.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:50.285088062 CEST	192.168.2.7	8.8.8.8	0xd6c4	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:50.451325893 CEST	192.168.2.7	8.8.8.8	0x2677	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:50.886739969 CEST	192.168.2.7	8.8.8.8	0x8a9c	Standard query (0)	privacytoo lzforyou-6000.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:53.158706903 CEST	192.168.2.7	8.8.8.8	0xe878	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:53.325818062 CEST	192.168.2.7	8.8.8.8	0x686a	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:06.256938934 CEST	192.168.2.7	8.8.8.8	0xd5c5	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:06.793525934 CEST	192.168.2.7	8.8.8.8	0x608e	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:06.960382938 CEST	192.168.2.7	8.8.8.8	0x5460	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:07.594818115 CEST	192.168.2.7	8.8.8.8	0x60e0	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:07.762376070 CEST	192.168.2.7	8.8.8.8	0xa32e	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:09.912467957 CEST	192.168.2.7	8.8.8.8	0x5cbc	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:10.077960014 CEST	192.168.2.7	8.8.8.8	0x8924	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:10.238271952 CEST	192.168.2.7	8.8.8.8	0x836e	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:10.412193060 CEST	192.168.2.7	8.8.8.8	0xb607	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:12.336947918 CEST	192.168.2.7	8.8.8.8	0xba18	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:12.519800901 CEST	192.168.2.7	8.8.8.8	0xdc50	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:15.609247923 CEST	192.168.2.7	8.8.8.8	0xd79f	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:16.722347975 CEST	192.168.2.7	8.8.8.8	0xa5c1	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:16.891743898 CEST	192.168.2.7	8.8.8.8	0x1943	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:17.067492008 CEST	192.168.2.7	8.8.8.8	0x68ef	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.104005098 CEST	192.168.2.7	8.8.8.8	0x68ef	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.274410009 CEST	192.168.2.7	8.8.8.8	0xcf9c	Standard query (0)	iyc.jelikob.ru	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.561086893 CEST	192.168.2.7	8.8.8.8	0x6bb4	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.751533985 CEST	192.168.2.7	8.8.8.8	0xf899	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.974908113 CEST	192.168.2.7	8.8.8.8	0x263e	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:19.146465063 CEST	192.168.2.7	8.8.8.8	0x9a05	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:19.165334940 CEST	192.168.2.7	8.8.8.8	0x572f	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:21.420629025 CEST	192.168.2.7	8.8.8.8	0x4e22	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:21.593507051 CEST	192.168.2.7	8.8.8.8	0x37b6	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:21.766551018 CEST	192.168.2.7	8.8.8.8	0x7b78	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:21.930042028 CEST	192.168.2.7	8.8.8.8	0x668f	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:22.109713078 CEST	192.168.2.7	8.8.8.8	0x1732	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:25.038505077 CEST	192.168.2.7	8.8.8.8	0x58ef	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:25.218506098 CEST	192.168.2.7	8.8.8.8	0x2ec1	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:25.408349037 CEST	192.168.2.7	8.8.8.8	0x45ae	Standard query (0)	sysaheu90.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:26.605974913 CEST	192.168.2.7	8.8.8.8	0xb18d	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 15:30:29.446518898 CEST	192.168.2.7	8.8.8.8	0x5c1d	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:29.817353010 CEST	192.168.2.7	8.8.8.8	0xbdb6	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:30.088576078 CEST	192.168.2.7	8.8.8.8	0x4911	Standard query (0)	hajezey1.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:40.996129990 CEST	192.168.2.7	8.8.8.8	0x8d4c	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:44.285001993 CEST	192.168.2.7	8.8.8.8	0xf71d	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:47.532489061 CEST	192.168.2.7	8.8.8.8	0x3d78	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:51.401598930 CEST	192.168.2.7	8.8.8.8	0x797d	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:54.618031025 CEST	192.168.2.7	8.8.8.8	0x1fa1	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:57.939132929 CEST	192.168.2.7	8.8.8.8	0x790c	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:58.008543968 CEST	192.168.2.7	8.8.8.8	0xcd8b	Standard query (0)	toptelete.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:00.902143955 CEST	192.168.2.7	8.8.8.8	0x641e	Standard query (0)	nusurtal4f.net	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.365901947 CEST	192.168.2.7	8.8.8.8	0xab88	Standard query (0)	znpst.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.565514088 CEST	192.168.2.7	8.8.8.8	0x9a5c	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.771392107 CEST	192.168.2.7	8.8.8.8	0xbc65	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:37.534353018 CEST	192.168.2.7	8.8.8.8	0x2dfd	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:45.136790037 CEST	192.168.2.7	8.8.8.8	0xe6e8	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:51.340296984 CEST	192.168.2.7	8.8.8.8	0x4e45	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:51.996310949 CEST	192.168.2.7	8.8.8.8	0x7e73	Standard query (0)	mas.to	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:54.816926956 CEST	192.168.2.7	8.8.8.8	0x193d	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:55.587068081 CEST	192.168.2.7	8.8.8.8	0xc53b	Standard query (0)	mas.to	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:58.992904902 CEST	192.168.2.7	8.8.8.8	0xa389	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:03.885279894 CEST	192.168.2.7	8.8.8.8	0x199	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:08.387541056 CEST	192.168.2.7	8.8.8.8	0x5645	Standard query (0)	telegalive.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:09.032435894 CEST	192.168.2.7	8.8.8.8	0x434f	Standard query (0)	toptelete.top	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:24.432200909 CEST	192.168.2.7	8.8.8.8	0xd7f7	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:25.501245975 CEST	192.168.2.7	8.8.8.8	0x46f	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:32.181284904 CEST	192.168.2.7	8.8.8.8	0xc784	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 15:29:50.276427031 CEST	8.8.8.8	192.168.2.7	0xe98a	Name error (3)	xacokuo8.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:50.304280043 CEST	8.8.8.8	192.168.2.7	0xd6c4	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:50.739317894 CEST	8.8.8.8	192.168.2.7	0x2677	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:50.906488895 CEST	8.8.8.8	192.168.2.7	0x8a9c	No error (0)	privacytoolzforyou-6000.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:29:53.178097010 CEST	8.8.8.8	192.168.2.7	0xe878	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 15:29:53.343168974 CEST	8.8.8.8	192.168.2.7	0x686a	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:06.637346983 CEST	8.8.8.8	192.168.2.7	0xd5c5	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:06.812875986 CEST	8.8.8.8	192.168.2.7	0x608e	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:07.443001032 CEST	8.8.8.8	192.168.2.7	0x5460	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:07.613675117 CEST	8.8.8.8	192.168.2.7	0x60e0	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:07.781887054 CEST	8.8.8.8	192.168.2.7	0xa32e	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:09.931878090 CEST	8.8.8.8	192.168.2.7	0x5cbc	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:10.097567081 CEST	8.8.8.8	192.168.2.7	0x8924	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:10.257822990 CEST	8.8.8.8	192.168.2.7	0x836e	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:10.431981087 CEST	8.8.8.8	192.168.2.7	0xb607	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:12.356302977 CEST	8.8.8.8	192.168.2.7	0xba18	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:12.537317038 CEST	8.8.8.8	192.168.2.7	0xdc50	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:15.634282112 CEST	8.8.8.8	192.168.2.7	0xd79f	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:15.634282112 CEST	8.8.8.8	192.168.2.7	0xd79f	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:15.634282112 CEST	8.8.8.8	192.168.2.7	0xd79f	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:15.634282112 CEST	8.8.8.8	192.168.2.7	0xd79f	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:15.634282112 CEST	8.8.8.8	192.168.2.7	0xd79f	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:16.741931915 CEST	8.8.8.8	192.168.2.7	0xa5c1	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:16.910960913 CEST	8.8.8.8	192.168.2.7	0x1943	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.121781111 CEST	8.8.8.8	192.168.2.7	0x68ef	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.293843031 CEST	8.8.8.8	192.168.2.7	0xcf9c	No error (0)	iyc.jelikob.ru		81.177.141.36	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.530072927 CEST	8.8.8.8	192.168.2.7	0x68ef	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.580732107 CEST	8.8.8.8	192.168.2.7	0x6bb4	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.771301985 CEST	8.8.8.8	192.168.2.7	0xf899	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:18.994231939 CEST	8.8.8.8	192.168.2.7	0x263e	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:19.165941954 CEST	8.8.8.8	192.168.2.7	0x9a05	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 15:30:19.192508936 CEST	8.8.8.8	192.168.2.7	0x572f	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:19.192508936 CEST	8.8.8.8	192.168.2.7	0x572f	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:19.192508936 CEST	8.8.8.8	192.168.2.7	0x572f	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:19.192508936 CEST	8.8.8.8	192.168.2.7	0x572f	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:19.192508936 CEST	8.8.8.8	192.168.2.7	0x572f	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:21.440638065 CEST	8.8.8.8	192.168.2.7	0x4e22	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:21.612938881 CEST	8.8.8.8	192.168.2.7	0x37b6	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:21.784255981 CEST	8.8.8.8	192.168.2.7	0x7b78	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:21.949590921 CEST	8.8.8.8	192.168.2.7	0x668f	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:22.127304077 CEST	8.8.8.8	192.168.2.7	0x1732	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:25.058145046 CEST	8.8.8.8	192.168.2.7	0x58ef	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:25.237951994 CEST	8.8.8.8	192.168.2.7	0x2ec1	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:25.827104092 CEST	8.8.8.8	192.168.2.7	0x45ae	No error (0)	sysaheu90.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:26.627618074 CEST	8.8.8.8	192.168.2.7	0xb18d	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:26.627618074 CEST	8.8.8.8	192.168.2.7	0xb18d	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:26.627618074 CEST	8.8.8.8	192.168.2.7	0xb18d	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:26.627618074 CEST	8.8.8.8	192.168.2.7	0xb18d	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:26.627618074 CEST	8.8.8.8	192.168.2.7	0xb18d	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:29.465260983 CEST	8.8.8.8	192.168.2.7	0x5c1d	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:29.836539984 CEST	8.8.8.8	192.168.2.7	0xbdb6	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:30.108221054 CEST	8.8.8.8	192.168.2.7	0x4911	No error (0)	hajezey1.top		185.98.87.159	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:41.015875101 CEST	8.8.8.8	192.168.2.7	0x8d4c	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:44.305762053 CEST	8.8.8.8	192.168.2.7	0xf71d	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:47.552169085 CEST	8.8.8.8	192.168.2.7	0x3d78	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:51.502931118 CEST	8.8.8.8	192.168.2.7	0x797d	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:54.637330055 CEST	8.8.8.8	192.168.2.7	0x1fa1	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 15:30:57.958695889 CEST	8.8.8.8	192.168.2.7	0x790c	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:58.029148102 CEST	8.8.8.8	192.168.2.7	0xcd8b	No error (0)	toptelete.top		172.67.160.46	A (IP address)	IN (0x0001)
Oct 29, 2021 15:30:58.029148102 CEST	8.8.8.8	192.168.2.7	0xcd8b	No error (0)	toptelete.top		104.21.9.146	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:00.921565056 CEST	8.8.8.8	192.168.2.7	0x641e	No error (0)	nusurtal4f.net		45.141.84.21	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		116.121.62.237	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		61.255.185.201	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		62.201.235.58	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		189.232.62.153	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		211.119.84.111	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		211.119.84.112	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		211.169.6.249	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		183.100.39.157	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		196.200.111.5	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:01.546233892 CEST	8.8.8.8	192.168.2.7	0xab88	No error (0)	znpst.top		190.140.74.43	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.584793091 CEST	8.8.8.8	192.168.2.7	0x9a5c	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.584793091 CEST	8.8.8.8	192.168.2.7	0x9a5c	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.584793091 CEST	8.8.8.8	192.168.2.7	0x9a5c	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.584793091 CEST	8.8.8.8	192.168.2.7	0x9a5c	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.584793091 CEST	8.8.8.8	192.168.2.7	0x9a5c	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.790961027 CEST	8.8.8.8	192.168.2.7	0xbc65	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.790961027 CEST	8.8.8.8	192.168.2.7	0xbc65	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.790961027 CEST	8.8.8.8	192.168.2.7	0xbc65	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.790961027 CEST	8.8.8.8	192.168.2.7	0xbc65	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:17.790961027 CEST	8.8.8.8	192.168.2.7	0xbc65	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:37.552494049 CEST	8.8.8.8	192.168.2.7	0x2dfd	No error (0)	api.2ip.ua		77.123.139.190	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:45.156213045 CEST	8.8.8.8	192.168.2.7	0xe6e8	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 15:31:51.359935045 CEST	8.8.8.8	192.168.2.7	0x4e45	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:52.015991926 CEST	8.8.8.8	192.168.2.7	0x7e73	No error (0)	mas.to		88.99.75.82	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:54.837757111 CEST	8.8.8.8	192.168.2.7	0x193d	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:55.605962038 CEST	8.8.8.8	192.168.2.7	0xc53b	No error (0)	mas.to		88.99.75.82	A (IP address)	IN (0x0001)
Oct 29, 2021 15:31:59.012947083 CEST	8.8.8.8	192.168.2.7	0xa389	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:03.904835939 CEST	8.8.8.8	192.168.2.7	0x199	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:08.407000065 CEST	8.8.8.8	192.168.2.7	0x5645	Name error (3)	telegalive.top	none	none	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:09.135754108 CEST	8.8.8.8	192.168.2.7	0x434f	No error (0)	toptelete.top		104.21.9.146	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:09.135754108 CEST	8.8.8.8	192.168.2.7	0x434f	No error (0)	toptelete.top		172.67.160.46	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:24.480983019 CEST	8.8.8.8	192.168.2.7	0xd7f7	No error (0)	api.2ip.ua		77.123.139.190	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:25.520663023 CEST	8.8.8.8	192.168.2.7	0x46f	No error (0)	api.2ip.ua		77.123.139.190	A (IP address)	IN (0x0001)
Oct 29, 2021 15:32:32.201045036 CEST	8.8.8.8	192.168.2.7	0xc784	No error (0)	api.2ip.ua		77.123.139.190	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bkhtxo.com
  - hajezey1.top
- qucostkxtw.org
- privacytoolzforyou-6000.top
- kslrhwirq.net
- vbyddwsgl.net
- ckkawpd.net
- qjhggbh.com
- yilaxxc.org
- mlylmiecm.org
- xquhxc.com
- lnvqewf.net
- xpqaga.net
- nxvperioa.net
- kclljmjl.org

- ifkorrg.com
- uknlp.org
- agijcahi.org
- fqyeks.net
- kmpicq.net
- nyssomocem.net
- wplogk.net
- uuiisjmkv.com
- siawn.net
- vvqdkujnt.net
- wogvus.org
- alsla.net
- bpoitfpcxi.net
- ryypml.org
- ifklliaybe.net
- omliatj.com
- sysaheu90.top
- ikgpguftl.org
- udluixh.org
- lbbxr.org
- toptelete.top
- 194.180.174.181
- nusurtal4f.net
- znpst.top
- dkukb.net
  - 193.56.146.214
- kvxhgwiwd.org
- fqytd.org
- dqqtfxwl.org
- knanvvmjy.net
- fmwfrtbvy.net

- ombhsev.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SkB6zJ6H3N.exe PID: 6372 Parent PID: 5472

General

Start time:	15:29:05
Start date:	29/10/2021
Path:	C:\Users\user\Desktop\SkB6zJ6H3N.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SkB6zJ6H3N.exe'
Imagebase:	0x400000
File size:	345600 bytes
MD5 hash:	B8D2D644A3AC5DF8AF9B3AFF803F3347
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SkB6zJ6H3N.exe PID: 6536 Parent PID: 6372

General

Start time:	15:29:09
Start date:	29/10/2021
Path:	C:\Users\user\Desktop\SkB6zJ6H3N.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SkB6zJ6H3N.exe'
Imagebase:	0x400000
File size:	345600 bytes
MD5 hash:	B8D2D644A3AC5DF8AF9B3AFF803F3347
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.308080762.0000000001F51000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.307863142.0000000000420000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3292 Parent PID: 6536

General

Start time:	15:29:16
Start date:	29/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000007.00000000.294055792.0000000003111000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: cviueca PID: 6216 Parent PID: 1104

General

Start time:	15:29:51
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\cviueca
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cviueca
Imagebase:	0x400000
File size:	345600 bytes
MD5 hash:	B8D2D644A3AC5DF8AF9B3AFF803F3347
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 97A5.exe PID: 6264 Parent PID: 3292

General

Start time:	15:29:52
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\97A5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\97A5.exe
Imagebase:	0x400000
File size:	345600 bytes

MD5 hash:	B8D2D644A3AC5DF8AF9B3AFF803F3347
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 97A5.exe PID: 5464 Parent PID: 6264

General

Start time:	15:29:56
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\97A5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\97A5.exe
Imagebase:	0x400000
File size:	345600 bytes
MD5 hash:	B8D2D644A3AC5DF8AF9B3AFF803F3347
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000014.00000002.368853755.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000014.00000002.368895221.00000000004E1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: cviueca PID: 6212 Parent PID: 6216

General

Start time:	15:29:57
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\cviueca
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cviueca
Imagebase:	0x400000
File size:	345600 bytes
MD5 hash:	B8D2D644A3AC5DF8AF9B3AFF803F3347
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cviueca PID: 6504 Parent PID: 1104

General

Start time:	15:30:01
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\cviueca
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cviueca
Imagebase:	0x400000
File size:	345600 bytes
MD5 hash:	B8D2D644A3AC5DF8AF9B3AFF803F3347

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

Analysis Process: cviueca PID: 2184 Parent PID: 6504

General

Start time:	15:30:08
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Roaming\cviueca
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cviueca
Imagebase:	0x400000
File size:	345600 bytes
MD5 hash:	B8D2D644A3AC5DF8AF9B3AFF803F3347
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001A.00000002.404074560.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001A.00000002.404878363.0000000001F51000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 5D4.exe PID: 5344 Parent PID: 3292

General

Start time:	15:30:09
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\5D4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\5D4.exe
Imagebase:	0x3b0000
File size:	512512 bytes
MD5 hash:	F57B28AEC65D4691202B9524F84CC54A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\5D4.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EDD.exe PID: 6868 Parent PID: 3292

General

Start time:	15:30:11
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\EDD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\EDD.exe
Imagebase:	0x810000
File size:	22528 bytes
MD5 hash:	787AF677D0C317E8062B9705CB64F951
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\EDD.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Analysis Process: 192F.exe PID: 3104 Parent PID: 3292

General

Start time:	15:30:13
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\192F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\192F.exe
Imagebase:	0x400000
File size:	212992 bytes
MD5 hash:	73252ACB344040DDC5D9CE78A5D3A4C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001D.00000002.419226513.0000000003190000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001D.00000003.402440778.0000000003190000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001D.00000002.419361924.00000000031B1000.00000004.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 80%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: 319A.exe PID: 4024 Parent PID: 3292

General

Start time:	15:30:20
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\319A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\319A.exe
Imagebase:	0xd50000
File size:	161280 bytes
MD5 hash:	9FA070AF1ED2E1F07ED8C9F6EB2BDD29
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\319A.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 43%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: AdvancedRun.exe PID: 4288 Parent PID: 5344

General

Start time:	15:30:22
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Analysis Process: 69B5.exe PID: 6140 Parent PID: 3292

General

Start time:	15:30:23
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\69B5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\69B5.exe
Imagebase:	0x400000
File size:	348672 bytes
MD5 hash:	539C39A9565CD4B120E5EB121E45C3C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000021.00000002.450724070.00000000047F1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000021.00000002.449678502.0000000002C10000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: AdvancedRun.exe PID: 5596 Parent PID: 4288

General

Start time:	15:30:27
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\0a4fc5b5-fef6-4ac6-8dad-72b92a431021\AdvancedRun.exe' /SpecialRun 4101d8 4288
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: 32BC.exe PID: 5540 Parent PID: 3292

General

Start time:	15:30:27
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\32BC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\32BC.exe
Imagebase:	0x400000
File size:	602112 bytes

MD5 hash:	D02C5BF9533CCE0E9EA3EAFC2F594A49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000024.00000003.442845982.00000000048A0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: powershell.exe PID: 4756 Parent PID: 5344

General

Start time:	15:30:35
Start date:	29/10/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user~1\AppData\Local\Temp\5D4.exe' -Force
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 4752 Parent PID: 4756

General

Start time:	15:30:36
Start date:	29/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: 6752 Parent PID: 5344

General

Start time:	15:30:44
Start date:	29/10/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 1432 Parent PID: 4024

General

Start time:	15:30:44
Start date:	29/10/2021
Path:	C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\3c9b9832-1586-402f-8df1-a3ced6cc50c2\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Disassembly

Code Analysis