ID: 553373
Sample Name: 0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
Cookbook: default.jbs
Time: 19:28:36
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

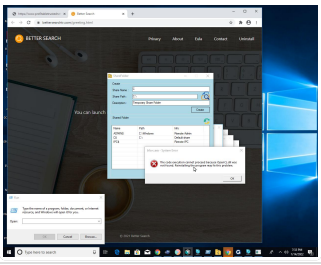
Windows Analysis Report 0CA57F85E88001EDD67DFF8…

Overview

General Information

Sample Name:	0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
Analysis ID:	553373
MD5:	971e01647fbdc05.
SHA1:	d8122ee820db5d..
SHA256:	0ca57f85e88001e.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

RedLine SmartSearch Installer SmokeLoader Vidar onlyLogger

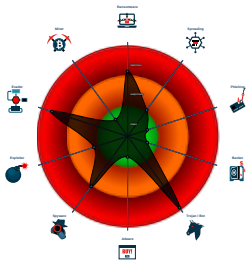
Score: 100
Range: 72 - 100

Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Yara Genericmalware
- Yara detected SmokeLoader
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- DLL reload attack detected
- Multi AV Scanner detection for subm…
- Yara detected onlyLogger
- Antivirus / Scanner detection for sub…
- Yara detected Vidar stealer
- Multi AV Scanner detection for dropp…
- Yara detected SmartSearch nstaller
- Disable Windows Defender real time…
- Found stalling execution ending in A…

Classification



Process Tree

- **System is w10x64**
- 0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe (PID: 7156 cmdline: "C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe" MD5: 971E01647FBDC05BEF3DF71B008E2CA6)
  - setup_install.exe (PID: 5976 cmdline: "C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe" MD5: 774F0D5B7DC3D2AD9CC4A0D921C9DA8B)
    - conhost.exe (PID: 6004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6548 cmdline: C:\Windows\system32\cmd.exe /c arnatic_1.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - arnatic_1.exe (PID: 5768 cmdline: arnatic_1.exe MD5: 6E43430011784CFF369EA5A5AE4B000F)
        - arnatic_1.exe (PID: 6732 cmdline: "C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_1.exe" -a MD5: 6E43430011784CFF369EA5A5AE4B000F)
          - conhost.exe (PID: 5348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 4964 cmdline: C:\Windows\system32\cmd.exe /c arnatic_2.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - arnatic_2.exe (PID: 4784 cmdline: arnatic_2.exe MD5: 68BC76A5DF7A7C5368E8AC9484584825)
        - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - cmd.exe (PID: 5868 cmdline: C:\Windows\system32\cmd.exe /c arnatic_3.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - arnatic_3.exe (PID: 6564 cmdline: arnatic_3.exe MD5: 208EF3505E28717F9227377DA516C109)
        - WerFault.exe (PID: 4104 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6564 -s 1112 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - cmd.exe (PID: 6576 cmdline: C:\Windows\system32\cmd.exe /c arnatic_4.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - arnatic_4.exe (PID: 6568 cmdline: arnatic_4.exe MD5: DBC3E1E93FE6F9E1806448CD19E703F7)
    - cmd.exe (PID: 6592 cmdline: C:\Windows\system32\cmd.exe /c arnatic_5.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - arnatic_5.exe (PID: 4816 cmdline: arnatic_5.exe MD5: 4A1A271C67B98C9CFC4C6EFA7411B1DD)
        - 4kmOewH8kDodZZ2lCCJUwR4o.exe (PID: 8116 cmdline: "C:\Users\user\Documents\4kmOewH8kDodZZ2lCCJUwR4o.exe" MD5: A9DED7D6470F741B9F4509863665F74C)
        - WN7mKI9_SQ4ujDwH_kKQHbe7.exe (PID: 8124 cmdline: "C:\Users\user\Documents\WN7mKI9_SQ4ujDwH_kKQHbe7.exe" MD5: 913FC52D517A4B4B2BE78103184EF87E)
        - l7AR_7u5i2RZzKoKItslndOd.exe (PID: 8132 cmdline: "C:\Users\user\Documents\l7AR_7u5i2RZzKoKItslndOd.exe" MD5: 0162C08D87055722BC49265BD5468D16)
        - R2IpdvMDW3mqJjP0F3OqthCG.exe (PID: 8140 cmdline: "C:\Users\user\Documents\R2IpdvMDW3mqJjP0F3OqthCG.exe" MD5: 5BF9D56B1B42412A2B169F3FB41B2A4D)
        - duCdI76Gqz3hAbP72ldEGd_3.exe (PID: 8148 cmdline: "C:\Users\user\Documents\duCdI76Gqz3hAbP72ldEGd_3.exe" MD5: 7A14B5FC36A23C9FF0BAF718FAB093CB)
        - bCyMoheCXfvXOWdcxUFW1mSl.exe (PID: 8156 cmdline: "C:\Users\user\Documents\bCyMoheCXfvXOWdcxUFW1mSl.exe" MD5: 6BFC3D7F2DE4A00FAC9B4EC72520209F)
    - cmd.exe (PID: 4020 cmdline: C:\Windows\system32\cmd.exe /c arnatic_6.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - arnatic_6.exe (PID: 6696 cmdline: arnatic_6.exe MD5: 08E6EA0E270732E402A66E8B54EACFC6)
    - cmd.exe (PID: 5692 cmdline: C:\Windows\system32\cmd.exe /c arnatic_7.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - arnatic_7.exe (PID: 6764 cmdline: arnatic_7.exe MD5: 614B53C6D85985DA3A5C895309AC8C16)
        - WerFault.exe (PID: 6936 cmdline: C:\Windows\system32\WerFault.exe -u -p 6764 -s 1092 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - cmd.exe (PID: 5344 cmdline: C:\Windows\system32\cmd.exe /c arnatic_8.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - arnatic_8.exe (PID: 6776 cmdline: arnatic_8.exe MD5: CFD5BF006F5EFC51046796C64A7CB609)
- rundll32.exe (PID: 5804 cmdline: rUNdlL32.eXe "C:\Users\user\AppData\Local\Temp\axhub.dll",main MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4140 cmdline: rUNdlL32.eXe "C:\Users\user\AppData\Local\Temp\axhub.dll",main MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - svchost.exe (PID: 2968 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s Appinfo MD5: 32569E403279B3FD2EDB7EBD036273FA)
      - svchost.exe (PID: 6924 cmdline: C:\Windows\system32\svchost.exe -k SystemNetworkService MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - svchost.exe (PID: 5924 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - svchost.exe (PID: 996 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s gpsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - svchost.exe (PID: 256 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s IKEEXT MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - svchost.exe (PID: 2320 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s iphlpsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - svchost.exe (PID: 2188 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s LanmanServer MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_4.txt	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	• 0x12b1:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\Documents\RcGzT5XRuDFwXkIj8ZcXjhgH.exe	JoeSecurity_Generic_malware	Yara Generic_malware	Joe Security	
C:\Users\user\Documents\RcGzT5XRuDFwXkIj8ZcXjhgH.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rtst1053[1].exe	JoeSecurity_Generic_malware	Yara Generic_malware	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rtst1053[1].exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000029.00000000.369507854.000001D91AAD0000.00000040.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x6546e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
0000002B.00000000.502724798.00000222CAB20000.00000040.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x6546e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
00000031.00000002.584879156.0000000002F70000.00000040.00000001.sdmp	JoeSecurity_SmartSearchInstaller	Yara detected SmartSearch nstaller	Joe Security	
00000024.00000000.339935983.0000027CA9C70000.00000040.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x6546e:$xo1: \x19%$>m=?"*?, m.,##"9m/(m?8#m$#m\x09\x02\x1Em ")(
0000002D.00000002.765127683.000000000580000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 33 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.3.arnatic_5.exe.3f90944.32.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	• 0x17f2c:$x1: https://cdn.discordapp.com/attachments/ • 0x18de4:$x1: https://cdn.discordapp.com/attachments/ • 0x1c3bc:$x1: https://cdn.discordapp.com/attachments/ • 0x1c9d4:$x1: https://cdn.discordapp.com/attachments/ • 0x1ca3c:$x1: https://cdn.discordapp.com/attachments/ • 0x1caa4:$x1: https://cdn.discordapp.com/attachments/ • 0x1cc44:$x1: https://cdn.discordapp.com/attachments/ • 0x1ccac:$x1: https://cdn.discordapp.com/attachments/ • 0x1d0bc:$x1: https://cdn.discordapp.com/attachments/
19.3.arnatic_5.exe.3f90944.79.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x17f2c:$x1: https://cdn.discordapp.com/attachments/ • 0x18de4:$x1: https://cdn.discordapp.com/attachments/ • 0x1c3bc:$x1: https://cdn.discordapp.com/attachments/ • 0x1c9d4:$x1: https://cdn.discordapp.com/attachments/ • 0x1ca3c:$x1: https://cdn.discordapp.com/attachments/ • 0x1caa4:$x1: https://cdn.discordapp.com/attachments/ • 0x1cc44:$x1: https://cdn.discordapp.com/attachments/ • 0x1ccac:$x1: https://cdn.discordapp.com/attachments/ • 0x1d0bc:$x1: https://cdn.discordapp.com/attachments/
17.0.arnatic_4.exe.d30000.0.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	• 0x12b1:$x1: https://cdn.discordapp.com/attachments/
19.3.arnatic_5.exe.3f8fd2c.31.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x18144:$x1: https://cdn.discordapp.com/attachments/ • 0x18ffc:$x1: https://cdn.discordapp.com/attachments/ • 0x1c5d4:$x1: https://cdn.discordapp.com/attachments/ • 0x1cbec:$x1: https://cdn.discordapp.com/attachments/ • 0x1cc54:$x1: https://cdn.discordapp.com/attachments/ • 0x1ccbc:$x1: https://cdn.discordapp.com/attachments/ • 0x1ce5c:$x1: https://cdn.discordapp.com/attachments/ • 0x1cec4:$x1: https://cdn.discordapp.com/attachments/ • 0x1d2d4:$x1: https://cdn.discordapp.com/attachments/
1.3.0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe.240787c.6.raw.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	• 0x12b1:$x1: https://cdn.discordapp.com/attachments/
Click to see the 37 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Svchost Process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara Genericmalware
Antivirus detection for URL or domain
Antivirus detection for dropped file
Multi AV Scanner detection for submitted file
Antivirus / Scanner detection for submitted sample
Multi AV Scanner detection for dropped file
Machine Learning detection for dropped file

Networking:

Yara detected onlyLogger

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara Genericmalware

Spam, unwanted Advertisements and Ransom Demands:

Yara detected SmartSearch nstaller

System Summary:

PE file has a writeable .text section
PE file contains section with special chars
PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

DLL reload attack detected

Malware Analysis System Evasion:

Found stalling execution ending in API Sleep call

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

Lowering of HIPS / PFW / Operating System Security Settings:

Disable Windows Defender real time protection (registry)

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara Genericmalware

Yara detected SmokeLoader

Yara detected Vidar stealer

Found many strings related to Crypto-Wallets (likely being stolen)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Yara detected RedLine Stealer

Yara Genericmalware

Yara detected SmokeLoader

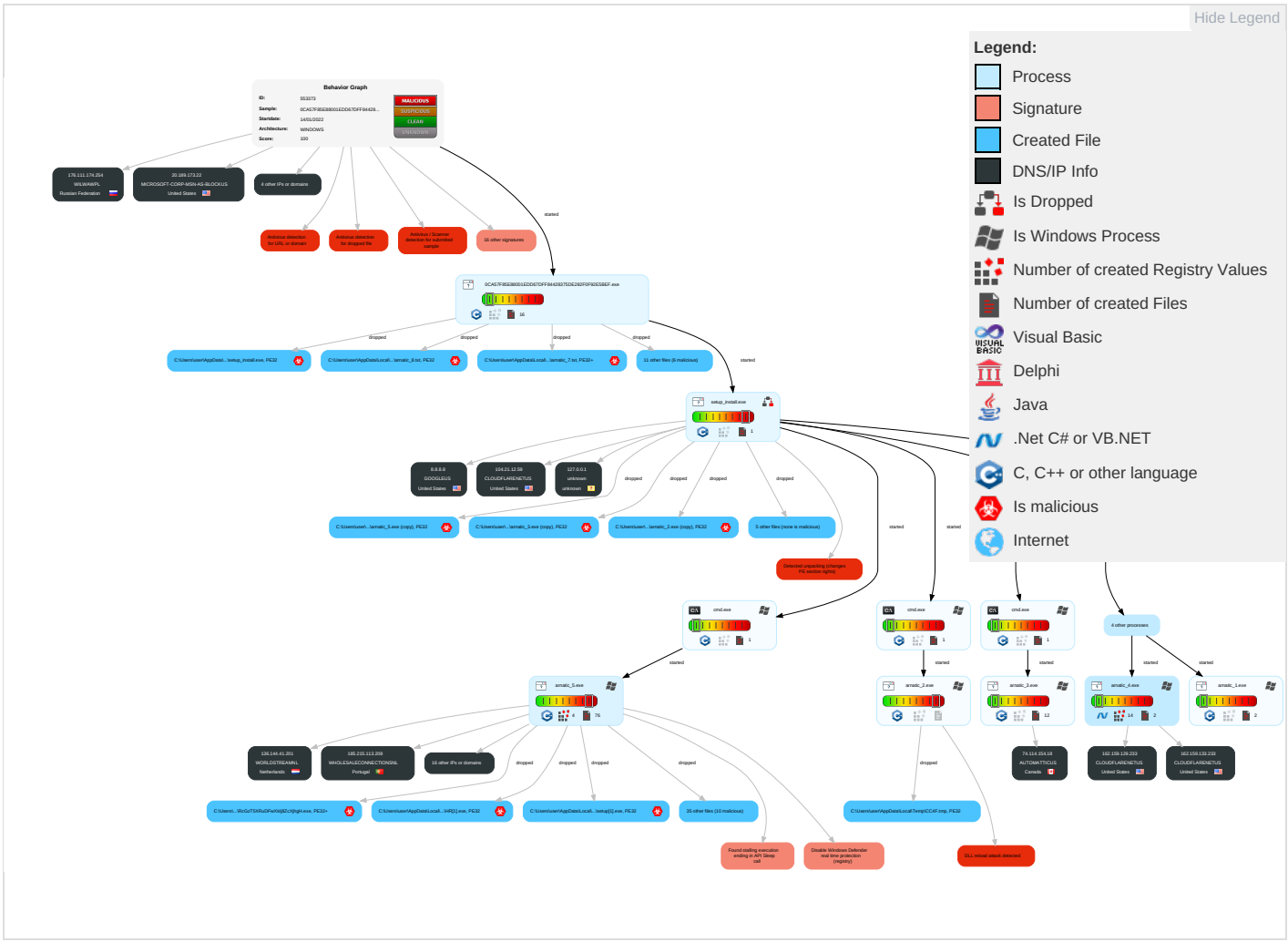
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts	Native API 1	DLL Side-Loading 1 1	DLL Side-Loading 1 1	Disable or Modify Tools 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Too Transfer 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Bypass User Access Control 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1 1	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 2	Obfuscated Files or Information 4 1	Security Account Manager	File and Directory Discovery 1 4	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Steganogra
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 4 1	NTDS	System Information Discovery 3 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonat
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1 1	Cached Domain Credentials	Security Software Discovery 2 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Bypass User Access Control 1	DCSync	Virtualization/Sandbox Evasion 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 1	Proc Filesystem	Process Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 2	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protocols

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protoc

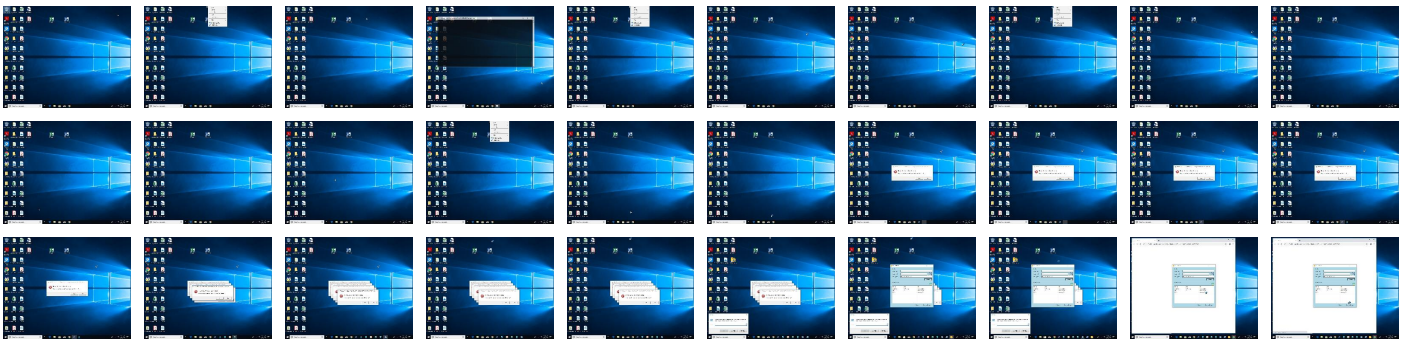
Behavior Graph

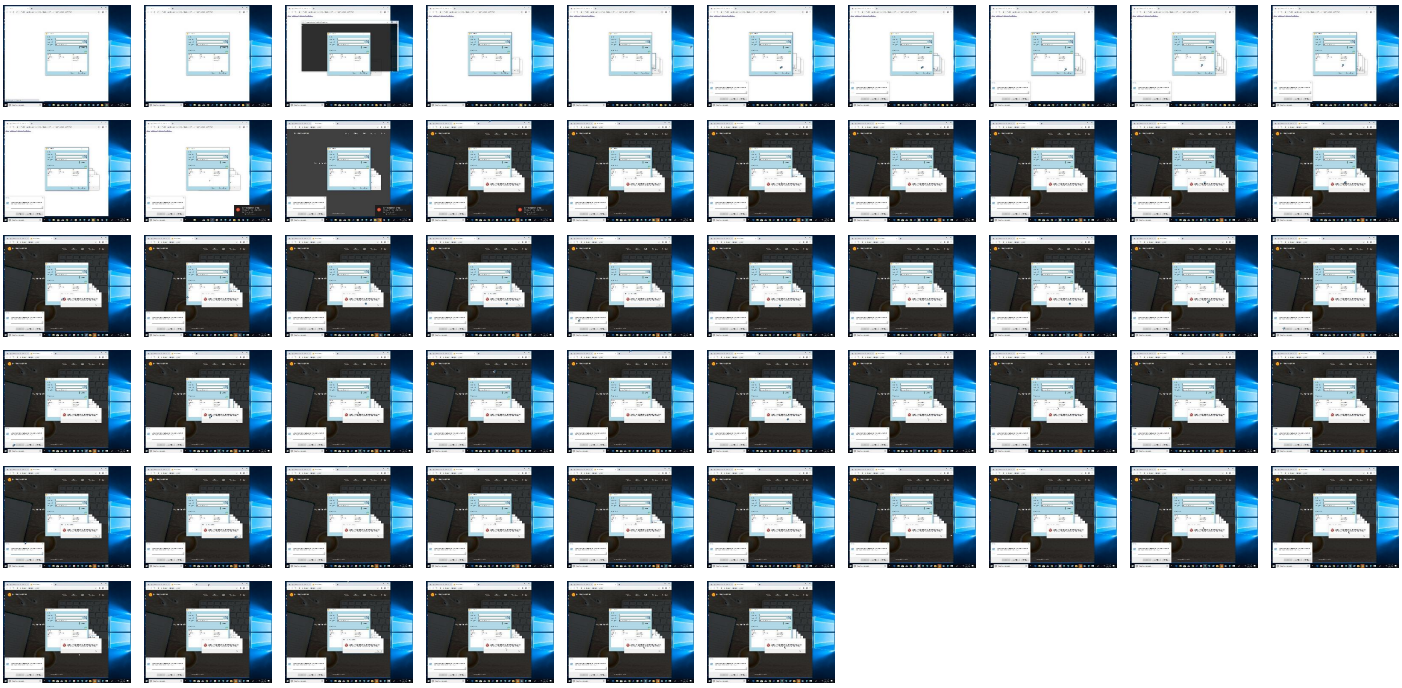


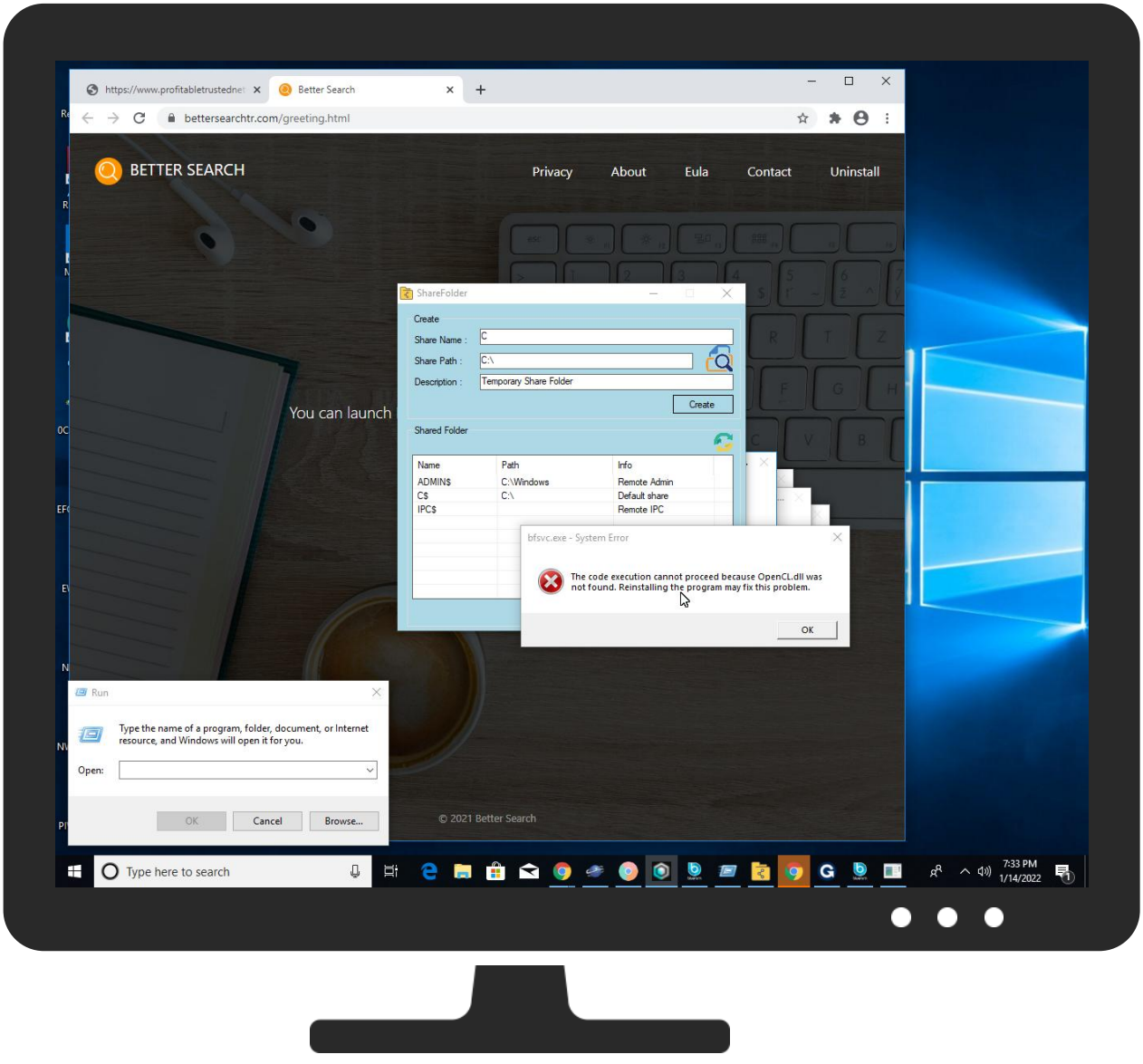
Screenshots

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
0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe	64%	Virustotal		Browse
0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe	11%	Metadefender		Browse
0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe	70%	ReversingLabs	Win32.Trojan.Azorult	
0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe	100%	Avira	HEUR/AGEN.1206449	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RobCleanerInstlr758214[1].exe	100%	Avira	HEUR/AGEN.1144918	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\HR[1].exe	100%	Avira	HEUR/AGEN.1142105	
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_3.txt	100%	Avira	HEUR/AGEN.1144344	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RobCleanerInstlr943210[1].exe	100%	Avira	HEUR/AGEN.1144918	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\searchEUunlim[1].exe	100%	Avira	TR/AD.MalwareCrypter.lssyq	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].exe	100%	Avira	TR/Redcap.loame	
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_1.txt	100%	Avira	HEUR/AGEN.1144071	
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_4.txt	100%	Avira	TR/ATRAPS.Gen	
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_7.txt	100%	Avira	TR/Dldr.Agent.ahsja	
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_6.txt	100%	Avira	HEUR/AGEN.1142187	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\search_target1kpd[1].exe	100%	Avira	TR/AD.MalwareCrypter.zmiqj	
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_2.txt	100%	Avira	HEUR/AGEN.1144344	
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.txt	100%	Avira	HEUR/AGEN.1202313	
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_8.txt	100%	Avira	HEUR/AGEN.1144344	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rtst1053[1].exe	100%	Avira	TR/Agent.grsnc	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RobCleanerInstlr758214[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_3.txt	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RobCleanerInstlr943210[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\searchEUunlim[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file4[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\appforpr2[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_4.txt	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file3[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_6.txt	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ferrari[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_8.txt	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\setup[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rtst1053[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].exe	23%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].exe	82%	ReversingLabs	Win32.Trojan.AgentAGen	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RobCleanerInstlr758214[1].exe	38%	ReversingLabs	ByteCode-MSIL.Infostealer.Generic	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\appforpr2[1].exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\appforpr2[1].exe	89%	ReversingLabs	Win32.Trojan.Azorult	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file3[1].exe	24%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file3[1].exe	64%	ReversingLabs	Win32.Trojan.CrypterX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.arnatic_1.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1144071		Download File
15.2.arnatic_3.exe.23e0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.0.arnatic_4.exe.d30000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
15.0.arnatic_3.exe.23e0e50.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.0.arnatic_3.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1143724		Download File
19.2.arnatic_5.exe.e20000.0.unpack	100%	Avira	HEUR/AGEN.1202313		Download File
13.3.arnatic_2.exe.9d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.3.arnatic_3.exe.2480000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.0.arnatic_3.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1144344		Download File

Source	Detection	Scanner	Label	Link	Download
19.0.arnatic_5.exe.e20000.0.unpack	100%	Avira	HEUR/AGEN.1202313		Download File
15.0.arnatic_3.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1143724		Download File
15.0.arnatic_3.exe.23e0e50.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.arnatic_2.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1144344		Download File
15.2.arnatic_3.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1143724		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.144.225.57/EU/searchEUunlim.exe	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file3.exemf	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr943210.exeI	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file3.exeme	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file1.exeC:	100%	Avira URL Cloud	malware	
http://xmtbsj.com/setup.exe	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file8.exeC:	100%	Avira URL Cloud	malware	
http://45.144.225.57/WW/search_target1kpd.exe/sfx_123_310.exe8	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file8.exe%d3	100%	Avira URL Cloud	malware	
http://45.144.225.57/WW/search_target1kpd.exemp	100%	Avira URL Cloud	malware	
http://joinarts.top/check.php?publisher=ww2&	0%	Avira URL Cloud	safe	
http://wfsdragon.ru/api/setStats.php	0%	Avira URL Cloud	safe	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr943210.exeg	0%	Avira URL Cloud	safe	
http://https://iplis.ru:443/1G8Fx7.mp3tData.phpr	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file8.exe	100%	Avira URL Cloud	malware	
http://tg8.cllgxx.com/sr21/siww1047.exev	0%	Avira URL Cloud	safe	
http://45.144.225.57/WW/sfx_123_310.exeKd	100%	Avira URL Cloud	malware	
http://stylesheet.faseaegasdfase.com/hp8/g1/rtst1053.exe	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exe	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file1.exeL	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file10.exe1d/	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file3.exet	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exeC:	0%	Avira URL Cloud	safe	
http://45.144.225.57/WW/search_target1kpd.exevw9	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file1.exe	100%	Avira URL Cloud	malware	
http://45.144.225.57/EU/searchEUunlim.exem	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file8.exeL	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file8.exeM	100%	Avira URL Cloud	malware	
http://tg8.cllgxx.com/sr21/siww1047.exe	0%	Avira URL Cloud	safe	
http://2.56.59.42:80/base/api/getData.php	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file7.exeC:	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file3.exen	100%	Avira URL Cloud	malware	
http://45.144.225.57/WW/search_target1kpd.exe	100%	Avira URL Cloud	malware	
http://joinarts.top/check.php?publisher=ww2C:	0%	Avira URL Cloud	safe	
http://2.56.59.42/base/api/getData.php	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file2.exe0.exeQd	100%	Avira URL Cloud	malware	
http://https://ipgeolocation.io/Content-Type:	0%	Avira URL Cloud	safe	
http://45.144.225.57/EU/searchEUunlim.exeC:	100%	Avira URL Cloud	malware	
http://https://curl.se/V	0%	URL Reputation	safe	
http://45.144.225.57/WW/search_target1kpd.exean	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exeI	0%	Avira URL Cloud	safe	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exeJ	0%	Avira URL Cloud	safe	
http://https://s.lletlee.com/tmp/aaa_v002.dllxxxxxxxxxxxxxxxxxxH	0%	Avira URL Cloud	safe	
http://212.193.30.45/WW/file9.exemZ	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file9.exe0	100%	Avira URL Cloud	malware	
http://https://iplis.ru/	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file9.exe	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file2.exeC:	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr943210.exe	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file4.exe	100%	Avira URL Cloud	malware	
http://motiwa.xyz/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://watertecindia.com/watertec/f.exe	0%	Avira URL Cloud	safe	
http://45.144.225.57/WW/sfx_123_310.exeW	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr943210.exeC:	0%	Avira URL Cloud	safe	
http://212.193.30.45/WW/file9.exeF	100%	Avira URL Cloud	malware	
http://stylesheet.faseaegasdfase.com/hp8/g1/rtst1053.exeC:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.209.157.230	unknown	Netherlands		18978	ENZUINC-US	false
176.111.174.254	unknown	Russian Federation		201305	WILWAWPL	false
172.67.177.36	unknown	United States		13335	CLOUDFLARENETUS	false
212.193.30.45	unknown	Russian Federation		57844	SPD-NETTR	false
212.193.30.29	unknown	Russian Federation		57844	SPD-NETTR	false
2.56.59.245	unknown	Netherlands		395800	GBTCLOUDUS	false
136.144.41.201	unknown	Netherlands		49981	WORLDSTREAMNL	false
104.21.5.208	unknown	United States		13335	CLOUDFLARENETUS	false
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
91.224.22.193	unknown	Russian Federation		197695	AS-REGRU	false
104.21.12.59	unknown	United States		13335	CLOUDFLARENETUS	false
148.251.234.83	unknown	Germany		24940	HETZNER-ASDE	false
162.159.129.233	unknown	United States		13335	CLOUDFLARENETUS	false
52.218.105.35	unknown	United States		16509	AMAZON-02US	false
20.42.73.29	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
45.144.225.57	unknown	Netherlands		35913	DEDIPATH-LLCUS	false
162.159.134.233	unknown	United States		13335	CLOUDFLARENETUS	false
2.56.59.42	unknown	Netherlands		395800	GBTCLOUDUS	false
34.117.59.81	unknown	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
103.235.105.121	unknown	India		17439	NETMAGIC-APNetmagicDatacenterMumbaiIN	false
74.114.154.18	unknown	Canada		2635	AUTOMATTICUS	false
188.165.5.107	unknown	France		16276	OVHFR	false
162.159.133.233	unknown	United States		13335	CLOUDFLARENETUS	false
20.189.173.22	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
194.38.23.114	unknown	Ukraine		40963	PRAID-ASRU	false
35.205.61.67	unknown	United States		15169	GOOGLEUS	false
148.251.234.93	unknown	Germany		24940	HETZNER-ASDE	false
185.215.113.208	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553373
Start date:	14.01.2022
Start time:	19:28:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 18m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.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:	43
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	7
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@72/24@0/30
EGA Information:	• Successful, ratio: 71.4%
HDC Information:	• Successful, ratio: 37.7% (good quality ratio 28.5%) • Quality average: 67.7% • Quality standard deviation: 41.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:29:50	API Interceptor	82x Sleep call for process: svchost.exe modified
19:30:01	API Interceptor	1x Sleep call for process: arnatic_6.exe modified
19:30:02	API Interceptor	2x Sleep call for process: WerFault.exe modified
19:31:05	Autostart	Run: HKLM64\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce system recover "C:\Program Files (x86)\java\Holyfybeshae.exe"
19:31:28	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run RegHost C:\Users\user\AppData\Roaming\Microsoft\RegHost.exe
19:31:31	Task Scheduler	Run new task: Telemetry Logging path: C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe
19:31:40	Task Scheduler	Run new task: AdvancedUpdater path: C:\Program Files (x86)\AW Manager\Windows Manager\Windows Updater.exe s>/silentall -nofreqcheck -nogui
19:31:40	Task Scheduler	Run new task: AdvancedWindowsManager #1 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 110 -t 8080
19:31:43	Task Scheduler	Run new task: AdvancedWindowsManager #2 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 111 -t 8080
19:31:49	Task Scheduler	Run new task: AdvancedWindowsManager #3 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 112 -t 8080
19:31:56	Task Scheduler	Run new task: AdvancedWindowsManager #4 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 113 -t 8080
19:31:58	Task Scheduler	Run new task: AdvancedWindowsManager #5 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 114 -t 8080
19:31:59	Task Scheduler	Run new task: AdvancedWindowsManager #6 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 115 -t 8080

Time	Type	Description
19:32:01	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run msuupd C:\Users\user\AppData\Roaming\msuupd.exe
19:32:24	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run msuupd C:\Users\user\AppData\Roaming\msuupd.exe
19:32:49	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\.exe
19:33:37	Task Scheduler	Run new task: Firefox Default Browser Agent 6ECBB60FBA9AB6D9 path: C:\Users\user\AppData\Roaming\jegdctt

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1234_1401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:RucQyfp3amzb8oRg/gnEzJyybdrS5JUoLXb+T:RucQytLnvg/gEzFxrS5JLQ
MD5:	0028D805C1F08B508639D640606FA76A
SHA1:	8CBF679A096986A379E3F26CC543BD52590D3514
SHA-256:	08BDF729CAEBE8EF33B5FDF0C39DB4FC8F15ED97B69E0C0F241A54C26810FF22
SHA-512:	1D30D7F41FDB514F5C4581E866D04D5AC8F71C2676EE89F3C8A2BADB8F0AA92B4A105F6734DE9F368C1E7CD908DC26AAFE20056EC026068E84E17ACD10D9619
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....Y\.....}.....].....}..... .....].....B.....].....}..... .....#5.....(.q.X...#K2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1234_1401[2].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1234_1401[2].bmp	
Encrypted:	false
SSDEEP:	12288:RucQyfp3amzb8oRg/gnEzJyybdrS5JUoLXb+T:RucQytLnvg/gEzFxrS5JLQ
MD5:	0028D805C1F08B508639D640606FA76A
SHA1:	8CBF679A096986A379E3F26CC543BD52590D3514
SHA-256:	08BDF729CAEBE8EF33B5FDF0C39DB4FC8F15ED97B69E0C0F241A54C26810FF22
SHA-512:	1D30D7F41FDB514F5C4581E866D04D5AC8F71C2676EE89F3C8A2BADB8F0AA92B4A105F6734DE9F368C1E7CD908DC26AAFE20056EC026068E84E17ACD10D961 9
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....Y\.....}.....].....}..... .....].....B.....].....}..... .....#5.....(.q.X...#K2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\LeGXxX6[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:fNIi1zBkFfpjq3Y4pIP2+nOX+34ZvqIZebM:fNIi1VkFfpjnnOZqM
MD5:	B3E391535619BA87B6FAA1BC245F1724
SHA1:	B1C05727CDE9C1A83D18457D62D2EBBF65BB3C3D
SHA-256:	65F8AD57031866ACCEE8E775A39FED5271EA31B4AC497AD350B8215E03161BD5
SHA-512:	5F8C83CC598E7064093A5F9BBADD8D713BDE70007F5745C4FE82808D9F76184768FFE9F2DDAC40C9F81BC1ED35070990473FC609D24B8F02A44E48AD30C4746
Malicious:	false
Reputation:	unknown
Preview:	...]....bb..%.....'..).P.%..P.....k.....}.....#.....C.. .....Y.....C.....=.....A....f..... .A.....\.....c.....c.....c.....c.....c....7....N.....c....6.....Wc....7..... c....6.....c....1.....c....6....j.....c....6.....S.....6.....M.....)....(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Roll[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:GrbLONBrbBrbCrbPlD6uxZBN3f/eri5lFBOcqyta/:GrfOrrdrurzR6uxZeriLmjyK
MD5:	113E473C4E083B156B202CB4F77F6C98
SHA1:	CAC119891DF6EE84AAC83FD1F75C856FB89D813B
SHA-256:	66E9645B2411B2D0207EE5F17D43CA5E8987DA684751A804C221A738D3E983CB
SHA-512:	10F7A2670DEA6EF80737C9FB2B8C6C7DE214B333950C684C24098CF4CBF072D8DE7F2CD72F05E02FECBA2DE0EA49993A22E6A2618D559CA1D53A647AD113E6 AD
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....1.....}.....q.....X.....q.....q..... .....].....q.....q.....}..... .....sZ.....U.4.N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3072:M1UJhFefM7JlXBTPGymqI3rfgusNKKSZrFE6dHo:vFUM7NGy2DmNvCH
MD5:	7A14B5FC36A23C9FF0BAF718FAB093CB
SHA1:	DC1244688756E1E10A73C1FCBD2FCA1C3AF3565F
SHA-256:	7A1481A3EC2646610CC068CE5BBCC169D75B7B664F3DF1997823A374B1CF19A7
SHA-512:	BFE06EDB9F1928C8F7923D7FD6D3766DFF272D06F61FC4C40F1A531589D161DE435631C8B53D5D02A64AE4BEE695FB47DF6467A5B117C188813BB0CE8BE565

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\f[1].exe	
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 23%, Browse • Antivirus: ReversingLabs, Detection: 82%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B../.qo|.qo|.qo|c.l}.qo|c.j}.qo|c.k}.qo|T.j}"qo|T.k}.qo|T.l}.qo|c.n}.qo|.qn|.qo|.qo|.qo|..m}.qo|Rich.qo|.....PE..L.....a.....r.....@.....0.....@.....$..... .....0...@.....text...7p.....r..... ..`.rdata..6`.....b...v.....@..@.data.....@....reloc..... .....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\help1201[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:5FC2E1AQ2Cj5XVwC1/eUGu2k543yn/jbngcYvI3T0pjC060Dbfe1kG:502E1Tzj5XmA/e1uDy+jrgcqOcfeOG
MD5:	421AC3D4E41572BCC8FD94C7D35A2011
SHA1:	41466FDE501D99965F70A279A40CC98FB73BE1D5
SHA-256:	DEB1B5F3163C30D36A3D4895E0A644F5FD4D7F560923D6370C2F286C0A8F1665
SHA-512:	E3A0B39774515F9E39D0DE38375B7B3DC55810A31CFB08572BEF526F5BD19282EEEDA9A1D721A90A1D161C62591E18BDED5BBC3CED2058A86DD46A8D2C3B4E1
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....E.....'..).P.%..P.....VO.7!..7!..7!..e...7!..e...7!...Z..7!..7 .h7!..e...7!..e...7!..e...7!.....7!.....W.....}.....=.....w.....i.....].....!.....].....].....w.....].....].....].....].....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\new_v11[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:SKwBtbUcuCYbLLWDNQqfIeB07ioYZp0ScY3okGC9a7FgpSlKxxB5lLFiiTI3SMTA:SBGJDWDKqfIG2ioYv0FC9BLpjU3bwzDb
MD5:	8D472A02F6F4FE76CA3CDDC66E862E2C
SHA1:	DB00C682662BFA9325F9C85F715263713B1E05F5
SHA-256:	AC91EA65EB63CB8FB9FBA0A47B05C01F62D11398BE75A6595439CF83E37B11FC
SHA-512:	A4327171533421F7E2C1E2DEF6EC9B9AFA855B37BDA4B83D38E523ECA119F7DCC914661B7F6F0C9E2C653828212601AC1DF461D84E84EBB0FD4649F7900999F
Malicious:	false
Reputation:	unknown
Preview:	...].....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L.....s.....}.....=.....1C.....u.....].....=.....}.....o b.a...[.....%..*Z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\real1401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:twGx7D2m17FHrZlitoE5xROme0yu6zE/tq5c8QT2LqG9QBc80jRPe2E:7n2mNFHrZVoYRbhn4E/tGbq8QS/jov
MD5:	7461DC699A0324B9627BFEF42F8997A6
SHA1:	233E80A76C67B4F61B3F75C007E8AD6CDC1BCD35
SHA-256:	8464ADC08481C39E3A3D633DBEF353A49838DA2825159CE273DD7346284FD46C
SHA-512:	CE88E9CAA4BF878098D230CE560594B4BDD56CE6D440BD2FCA02AAFF082899E23111C74A416C5E883BB50B6B3B8C099FD68EBF2CCC0C38E62E4ED1A04A3AF800
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\real1401[1].bmp	
Preview:	...]..........bb..%.....E.....'..).P.%..P.....D...D...D._D...D..ID2..D.%.D...D...DT..D..ND...D..^D...D..[D...D.....D..... i.....}.....5...-.....}.....].....=.....Q.....9.....].....i...=.....#:.....5..... .....T...].....1.....].....Y.....].....w....=.....[.....].....-.....].....].....K..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\russ[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:3En3cQyfp3amz3/b+R2qtz6EGEzytnJ/AevLrap:3O3cQytLf+v5DGEzytnhAeH+
MD5:	9A318136E1125B55215EF5138044BA60
SHA1:	E797F2E3A14E1EA47817F92EDC792E0A8D440C09
SHA-256:	F8D62C83234CE668E787BBC4CD785929A94CFCFD65027B79AF2574F4D94C7371
SHA-512:	FE735DB74F56E03AC65D111CAC39E952367A74426E3FE93596BF9F7EE3B2D9CD5188905FBD982C0DCDF5E59DA37EDA1A0AA25439FE7D865DE60A15BC3F71D 8A
Malicious:	false
Reputation:	unknown
Preview:	...].....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....-.....}.....>.....A..... .....].....x.....].q.....}..... .....R.F..].P.Y.....{...t...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\softer1401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	49152:RfucQyVj4K7efDARM9hCIzd24U1xe0om7kc8lbbTtq:RfayVjF7efDhYmd2hje0Joceftq
MD5:	2172158FCA5FF61D086C7C9758E6317A
SHA1:	1A2C933ADA88036A19A4E39C613B8120DA471147
SHA-256:	F216E94249C77DEEA8567A9D6A5C45F52A5F27135EDD22F58DC0DA5E27C44533
SHA-512:	D76212393B1A596FC18D6B1C1537E1F2DA86C0C5315FEB77639B83C727C5F3337900EC78B97DE4735C960754A5C8951DBBE3C8E2A43649E95F6D9E48B485263
Malicious:	false
Reputation:	unknown
Preview:	...].....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....A.....}.....=.....=..... .....].....n.....=.....g.....}..... .....X..O..K..t.}B..../...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\utube0501[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	98304:0E6U8CakDBZapwJeLm+fKTMsdkUwVOfKNVeS6t9IGW/2InyF8pcDK0CjezHfQT/1:0jbClhYJKTvkUaVeSK9PtZ8qLowQuAF/
MD5:	3415D918A3144E485AC7B55DF36C480A
SHA1:	F7EE383DC873E629690A83E197250713F2CCB8E6
SHA-256:	28EAEE74D58DEB0B1AC344C924FACDB1F9CA2C7CFB675E05D9E15CBEDC72D2E0
SHA-512:	12F958617B99D353FBC2EDE5461E869A7DB12863C89B043382B9FB125DE2D07956126DDB2AE2C38DC541B7B234DC48864639F36EA3A309D8F15650D42DA4608
Malicious:	false
Reputation:	unknown
Preview:	...].....bb..%.....u.....'..).P.%..P.....@|.....2;.D.....2;.I..kkD....kkp.....j.x.....}.....-.. .....-.....yt.....-..e.....w.....-... .....y.....].....]..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\newt[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\newt[1].bmp	
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:dl3cKvQB7bXXCx7il1PUYM91pEhTCbKRlsIhYFfL:dlGB77XCx7iHS9/EhTCmRlrYFD
MD5:	4A07E2790DDBE0A071C9753A35789156
SHA1:	71A0F9CD6605E82310B2A9DB71EECF6032B52B93
SHA-256:	5347691898EE93E549D9AFA5BA870FF736A7EC7DF72527A177E8670B176508FC
SHA-512:	3F1C06E367B2B650201B0E864249CD9DBF9A801E4AAB922D01E7AAE60EBF28EF2B9B8C902AF3C9DE75779C749F8C865D33869E8FD7BFBE280798EBD62822CD9
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....'..).P.%..P.....).....)...v.).....).....O.....O.k.....O.....}.....}.....M.....}.....=.....a..9.....U*.....M.....}.....}.....}.....}.....}.....9.....}.....}.....%...3.....}.....}.....}.....=...m.....}.....g.....}.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\stalkar_4mo[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	49152:jBSz4y+TUB5AO5beZlmbwtpjRpzFEPszp1Rmv6mgREVUuaLfF7HId:j+pMuFJM1p5EkzpPm6xREVUBod
MD5:	936909AFD56C9E5A07A8611F751FF9CF
SHA1:	6CF7E70FA290D73322C3597BE8F693805B7E23D7
SHA-256:	F2A9256FB949A42729FC4764BEDF6F3669D942ED022FD7B9A316998B9B35ACC6
SHA-512:	9308E460DF9DB91970B086C8F99AFE50246CF995C47AABE580514172484F5456F096AE1E26D89DBCD85BABE52B6AE5AA8CDACBC5E0FE813EFFE975104AE132DD
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....'..).P.%..P.....D.....m.....M..... ....}....q..M.....q....m.%.....!.....e.....}.....}.....}.....]..... .....CTW'.... <g...1.....1....e.e.....i..W..`.e.....q....]S..I.(W.{..u..|.3-|....a*..x...r.%.eH.!.....+u). .0...Y9.u..u...>t;....|R?A#..Dh..I.ia..V.<.....$.Wy.k`.S.W#z,...}....E..B.:gqD.....^./h.....tn...W .....V..i.S..:.|.T.....6JS.}gC8E*{..%.rZ[h..rw"..>...6.....c=...J..~tjBU7.....Djm.s.>n...6.P`C5s.0..|. ..E..P.....8.<..;gqj<p....1^.....I>..f.A.....IBs.K.yFT^..X.:....=.8..>.B..A..... H.B.E:....F.....~..Qq....?....8.<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RobCleanerInstlr758214[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	1536:nf7EzXSAH/axBSy+zotG3xKapfZVYB4gfOKKKKkcsHgcsV1JRJn2Qx:nf7EzCAHyXe0tG3ZBZVYfb5HNsV1c4
MD5:	0C70224F09C65619BC9D6AFC456294C9
SHA1:	975AA4311B2C4FEDE2DB8BD6293F5C54224348C7
SHA-256:	AC0B18AE0851CF5CB499BDCBA6BCE5D260F114768425AEED65CF6086B27A323D
SHA-512:	B72C10B8A3ED94E6E7796A562F860B9AD8F3815A3F3B9A24B98C56BD77A5318EDDCF69E41ADAD5975206C04E220107DF65BABDABF9DB98831BA567947B7936 2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e.....0..... ....@.. .....F... ..@.....S.... ..H.....H.....SH..RSn.|J... ...L.....@....text...`.....P..... ..`.rsr c...H.... .....@..@.reloc.....@..B..... ..`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RobCleanerInstlr943210[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RobCleanerInstIr943210[1].exe	
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3072:CwM8ll/9+Qa/PHsuH3EbSSSSSabsZGpu:9nQQQacuqSSSSSabsZG
MD5:	A9DED7D6470F741B9F4509863665F74C
SHA1:	FF1A2ABB33D9DD290C9349565586C6C1E445DC1E
SHA-256:	2F326116DF411C1C9AA3728E0C191FD0888FF63DB7DB08CC70DB1F1AEBE88347
SHA-512:	507D729DDC2533616A6DF372BB8C175D44DC5B68D0A455496DE34019FCF685A6EF6A36693CCB9417637CB9783CFD48EDB039274A7C51476FD39F98796B1D78D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.....0..... ....@.. .....N.. ..@.....S.... .....H.....`_...&.tJ... ...L.....@....text...`.....P..... ..`.rsrc..... .....@..@.reloc.....@..B..... ..`..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\appforpr2[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:EbWxj7XagNorsFTCp64vSMLjYgrkhnuzbgwu:2Wx3a1kO6SS6c9unn
MD5:	0162C08D87055722BC49265BD5468D16
SHA1:	901D7400D1F2BC4A87EDAFD58FEBFAC4891F9FE8
SHA-256:	92F1DF4DBB0E34C38083BB9516FB5C812175B5B73C9FDA81CA8047C5C38A1ABB
SHA-512:	193A12BAF5819BC58B310BFCC5E33EEDD06C130922596A6A4F8A16BC705A28FE3D8E75C689ECFBB970F21D66FEFA7830108F661F0E95586B4D87D1DEFB85A05F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~...-...-..-..{-...-..m-...-..j-...-.@.-...-...-...-..d-...-..z-...-...-...-Rich...-..... .....PE..L...I.`.....0....@.....@.....U.....]..P....p..X.....1.....P..@.....0..... .....text...#..... ..`.rdata..b7...0...8.....@..@.data.....p.....T.....@....rsrc...X....p.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ferrari[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:NPfr7cLGO+vNNeB/b39qxwL9AtxansJWBpB2Ol1acxTWwnWQL:Nr7cLGvIB/ExPxPcjBrl19TW9a
MD5:	5BF9D56B1B42412A2B169F3FB41B2A4D
SHA1:	E52BA18C693843BB1A72FCA134AFBDE40A0568DF
SHA-256:	02D1BCDDD657EC1F5C83A8420E6C30FC2A83980FFCC05A0C3BB9CFA70ED1FA06
SHA-512:	E87CA5E5F7CBEF70A275C1294C3E9FC27B35A370C01F17CA84E22C99381BD96E7DDC89748D6A12D069B013E93FE2C60FA810EC98C6C4EEC864E8D1B2EF0EF1F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W.7,..(~W.Rich)~W.....PE..L...#:._.....k.....@.....P.....(.....@.....@..... .....L.....text..... ..`.data.....@....nan.....@....dis.....@....fubah.....@....rsrc... (.....@..@.reloc..hG...@...H...T.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file3[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file3[1].exe	
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:t8f39B+OecSnrJYG4oPSidpXPQvzJetHu7MgUEjumXKHt:worJYGPd1PQ7JUaMjEygK
MD5:	2DBF77866712D9EBD57EC65E7C1598A8
SHA1:	25693E771D3D25112FFA7C38875DECD562AC808D
SHA-256:	2E382DCD1F433490E453D5E7E710D2BB821C2DF09F1E16B675EE060D46DA80D6
SHA-512:	609AA7242A8908AD7B59FD5F303492DDF435320106219D9E35F88B6A9976ADC72CA1E72CD17F714D349E430F8A0D330837C81AD947AC62E4DCD2C83D32A2DB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 64%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.........+..R...d:.....Q..... ....PE..L...P.....0.....F..... ... .@.....+.....@.....0.....@...D..... ...data.... .....`.shared.....0.....@....rsrc....D...@...D.....@..@.CRT.....x...L.....@..... .....kg...}R..hI.>..H......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file4[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:CLw0gZFUJuzEpCMQaVQ3luptUH2jQ66PYTnxRcqh+ZygmiuLscbTzAIIbasU+By:mPJOqppLUHWP6PY7xRUjAocF+Fn
MD5:	399A7496E00DAC0E986FB7E4842E6A2C
SHA1:	8C837A80329CD1894050AE8163881289A971A99E
SHA-256:	7747F0397EF330B53D0BD68DFE9ED416A935851760657B7DF0ED93A7A8A5692C
SHA-512:	75B3467BC465E7AC9841E6A742A21373F2A044C0266C388B7BB63331ACEE73E05EAA329E4B3A700FF1EEF0C85D84F128D72D119B5018A1B29C88E29B8589D8E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....>.... .....@.. ..... @.....W..... ....H.....text...D.... ....`.rsrc.....@..@.reloc..... .....@..B..... .....H.....$7.....PD.....t.....g.....y....(.E..*.s.?...W...**....(i...*f....(j...r7..p(....(k...*f....ol...(m...ol...on...*.sCD...\| ...*f....ol...r.#.p(....on...*f....o....r.#.p(....on...*f....o....rO$.p(....(k...*.....o....r.$.p(....r...p(....r-..p(....(....on...*f....o....r4%.p(....(k...*f....o....rv%.p(....(k...*f....o....r.&.p(....(k...*f....o... .rk&.p(....(k...*.~....:#...r.&.p(.....#...(....o....s.....~....*.~....*.~

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rtst1053[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	49152:7rEOLD0xW+aJVXfxu3Eosp/qw7RV+uY/:023Jtosp/qw7yb
MD5:	DD3C57E2520A47D634E5FAAC52782FDA
SHA1:	73AF831AA23F72D82FE80E84B0C4411E6A9DCCB6
SHA-256:	03B887397102E717DE5EF8A0D4D0374BDF5347A85DDDC8C829714770142B8FDF
SHA-512:	37F0BE02B923B873DAA2CB98A49C42A1AB2DCB3B9A5422E7B5FECFEDF1A90CE2F00E375A41C1C0331A4B3E3B96B5FBDC267907966AA8406DED1970B42F3E6 2C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rtst1053[1].exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\rtst1053[1].exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....i..-..A-..A-..A9..@8..A9..@ ..A9..@...A...@...A...@,..A...@=.. A...@'..A...@...A9..@$..A-..A..A...@%..A...A,..A-.pA,..A...@,..ARich-..A.....PE..d.....a.....".....}.....@..... !.....`..... .....DJ..d.....J.....`..... ..#.. :..p.....:..(...:..0.....8.....text..... ..`.rdata...[.....\.....@..@.data.....`..^.. .N.....@....pdata..`.....@..@_RDATA.....4.....@..@.rsrc....J.....L...6.....@..@.reloc...#.... ..$.... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\searchEUunlim[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:Ab0yasxDZDYbVJU9Dwsn/m5eo7CKS6O4gySTePDyB9nb41xqGONesE:AYZKlUbVJeEYu9OVxePmBix/aE
MD5:	6BFC3D7F2DE4A00FAC9B4EC72520209F
SHA1:	0DC92779C7BB4C9D6C3A02FFA176199F652B3976
SHA-256:	B039B93D8CF1911397F74A703784D69363544F97F059266256CBAF419E8B2C3E
SHA-512:	DB92E098F611742A38F4B0BA5C202CE48AD926C51A6396FFEDDBC8C75891F4E104558AF7D9D108CC197BEA3CFFFDEDFFD99A9E24AD481350FA5A71DA80166 7B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#X.g9..g9..g9..yk0.v9..yk&..9..@...d9..g9..9..yk!._9..yk1.f9.. yk4.f9..Richg9.....PE..L.....L`.....2.....0O.....P....@.....-.....-..(.....~.....p.....`...@..... (.....text....0.....2..... ..`.data.... ...P.....6.....@....bot.....p.....J.....@....zuxi...K.....L.....@....tive.....N.....@.. ..roduwe.....P.....@....rsrc.....^.....@..@.reloc..8;.....<.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\search_target1kpd[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	1536:a6x3MUH9LNxYEThBPnt21SnmymczorCtMqvJK2uHjmUKKDfj/RhsN:acL5T78UnmDGJuHjmUKKzrRhs
MD5:	3F13A6A1BBCEC7D68C15DEE4EEB7DF58
SHA1:	9DC2468D6E9E61D572D4C1A54B3C80DD69FF2287
SHA-256:	17D8AA92EB9BDA31A05D0BD15A52734B18AE72C9F4B6EFEF628DD5773E0F71C2
SHA-512:	E1033871C72422E80132C0E5DECE0FCBD0B9279374BC84330A3899DFFE5E94D5AFD637D45C0949D7FB775EFE07A195CB924FA9D099D2AF1A660B9A80F08807E F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Ntu.....G..-....G.....G..b...-.`.....G.....G.....G.....Ri ch.....PE..L...!._.....w.....@.....pw.....t...<.....v.....@..... .....text..... ..`.rdata..x.....@..@.data...$.s.....@....joy.....v.....@.....@..@.rsrc.....v.....L.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\setup[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:HCA2YLo85KNa/jA6p8MIQfJFDrJoYkLLTE:HX2ImN4F2MTJFBoY04
MD5:	913FC52D517A4B4B2BE78103184EF87E
SHA1:	5ECF0E1AF77F229C46F13B9C4FB6341761ECD818
SHA-256:	734D3D7D77B4FAD43FF22B081E664D6CFEE09C67AEC8F81CFA524924CB7785FA
SHA-512:	1881476719098573F618A4FFB21EC6729E8B72A869AAE7D959EAF49DF5A085208F1DADFBA71ACC71A4FCCE5046FE2863A7C19EEBA04A36F13564059B23E60733
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L..../._.....P.....@.....p.....t...P.....(.....@..... .....L.....text..... ..`.data.....@....ruceg.....@....todako.....@....godol.....@....rsrc.. .(.....@..@.reloc..ZF.....H.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\27f_1401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:rflvzk/CDajDJO4kUDdfL5Br+j6aSTJQPuh/ZnE1hZ0DQUiBs6wQkcI3Jlee7H:rlv46OHgUDdD5MjXSTJwuhBnE1L0DQUA
MD5:	BF2EACD3AC9C12709881AA852DC60358
SHA1:	EEBE60C4775143199D1EB1F63D48675B45CCC289
SHA-256:	48B201629679F0E035CA613F27B1170CBEC03FC7975A5A6D789DCF6B8B926526
SHA-512:	E116F250E6CFEC842AC62DFC37FA8135BDDBC854FEF4D87C54DE876A384E52ACEF18D22703F4AC83C5EF82EA9AB1E5DD0A935C574F0B5AE8FF8A28B55AC026E3
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....}....'..).P.%..P.....8g.Q|...|..|...bTZ.f...bTL.....[.....|.....bTK.F...bT[.}...bT^.}.....|.....+.....}.....m...1.....-#.....lv.....%.....q.....r.....m.....T.....i.....].....M.....].....w...}.....].....m.....].....%n.....'.....?.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\HR[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:8Qi3uAIKMYqN96m6UR0IrELWKlVwlpkTyL6Ka3EjiqxyNefotS10m:8Qi+PvNgHIALfGHkTVwiPk4Bm
MD5:	3A9664DAD384F41DCDC1272ED31171E0
SHA1:	D525F290DCF469F5B26654A4DB685092F8616509
SHA-256:	A85903FC9F06B4CCC4136FC573F6AFDFB6B90D555530F7259E4E8CB18616B724
SHA-512:	F7C3E6D561DF34C63E373C6CC715E1C13AB68013360F1694EEFAE6C896345ABD1135E60B5AA5D96FFD245AB7D24C9D856A7EAB58C9798D3B7B355E9DE161830
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....@.....@.....@.....P.....CODE....0..... ..`DATA....P.....@...BSS.....idata..P.....@....tls.....rdata.....@..P.reloc.....@..P.rsrc.....@..P.....@.....@..P.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\redcappes_crypted[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	98304:1K7AC3AO28pjeXPl8XlY9tBe0Mle44y4I:UlQz8paflsYzBfMlx4Vl
MD5:	07F5A548B1C79C6FCE9EEBA1A13CA8D4
SHA1:	3C6459995AB858E5C0283B62A904F91E64CF111F
SHA-256:	FCA4E91292EAE5B06BCFFDFDCB043346996A74BE2686C9C2E3CB9FF517E59110
SHA-512:	3F95790701C20BB631B9A7CFDD5A99F1BC10862703F142D0F16EC80BEFAFD804B1B261719999B105FFC6E62575875F9054915F592645A3783D5C4AE21DB27C14
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....'..).P.%..P.....g.}.....}.....M.....?.....}.....}.....m.....}.....}.....c.....}.....M.....k.....}.....-.....9.....}.....-.....-.....}.....].....{.....}.....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_1.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	729724

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_1.exe (copy)	
Entropy (8bit):	7.767862089624224
Encrypted:	false
SSDEEP:	12288:CcXe9SLN+NH0khUZY+vcvw15G8QYewwB9gL1xB3iJZcaFh:CcO2Q2ZYuloel9gLHB3yZcaj
MD5:	6E43430011784CFF369EA5A5AE4B000F
SHA1:	5999859A9DDFCC66E41FF301B0EEB92EF0CE5B9F
SHA-256:	A5AB29E6FC308D1FE9FD056E960D7CCD474E2D22FB6A799D07086EC715A89D9A
SHA-512:	33EF732056182B9AB073D2EACFD71D3F1CB969EE038A19336FB5E0263A4E870742082C756A57010A26E7EAB747A2332523D638F2570B8070B933BF957D2DEA96
Malicious:	false
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........3...`...`...`...`...`...`...`...`...`...`...`..`...`...`...`..`..`...`Rich...`....... .PE..L...0..`.................`...p......d%.......p....@.........................................................................Pz..d.......<...........................................................................p.. ........................... text...._.......`.................. ..`.rdata..z....p... ...p.............@..@.data....5.......0.................@....rsrc..............................@..@... ....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_1.txt	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	729724
Entropy (8bit):	7.767862089624224
Encrypted:	false
SSDEEP:	12288:CcXe9SLN+NH0khUZY+vcvw15G8QYewwB9gL1xB3iJZcaFh:CcO2Q2ZYuloel9gLHB3yZcaj
MD5:	6E43430011784CFF369EA5A5AE4B000F
SHA1:	5999859A9DDFCC66E41FF301B0EEB92EF0CE5B9F
SHA-256:	A5AB29E6FC308D1FE9FD056E960D7CCD474E2D22FB6A799D07086EC715A89D9A
SHA-512:	33EF732056182B9AB073D2EACFD71D3F1CB969EE038A19336FB5E0263A4E870742082C756A57010A26E7EAB747A2332523D638F2570B8070B933BF957D2DEA96
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........3...`...`...`...`...`...`...`...`...`...`...`..`...`...`...`..`..`...`Rich...`....... .PE..L...0..`.................`...p......d%.......p....@.........................................................................Pz..d.......<...........................................................................p.. ........................... text...._.......`.................. ..`.rdata..z....p... ...p.............@..@.data....5.......0.................@....rsrc..............................@..@... ....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_2.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	248832
Entropy (8bit):	6.384824159424914
Encrypted:	false
SSDEEP:	3072:jBNmLqpxDPt+pt1VPA9TRtQuTqLWe5fJZhuCQm+1yUVNSmE:tm0yt1VP0guTqFJSbmJUSt
MD5:	68BC76A5DF7A7C5368E8AC9484584825
SHA1:	8523D1CD6709B58F7ACE6EE6F08343DF6BFFDBDF
SHA-256:	E5171BF897A4D8C420708E09D1DB070A185EBAC7010E17AE7695541C383A95DB
SHA-512:	C2320BEE41FFD37CB945AC131578A3F873B4BB5FD6D46BBA6DCEFD061946E3359F7F95D4DB5FA18C20E8DB602AFC8D53824D18AFA6643AAA58A9B2BD2D8C8 1EE
Malicious:	**true**
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........"0..C^.C^.C^....C^.....C^..%.C^.C_..C^....C^....C^....C^....C ^.Rich.C^.................PE..L....?v^......................X..................@...........................Z.....................................0...J.......d.....X......................@Z..... ....?..@......... ....text...z........................... ..`.data...P.V......N.................@....rsrc.........X.....................@..@.reloc...I...@Z..J.................@..B.................................... ....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_2.txt	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	248832
Entropy (8bit):	6.384824159424914
Encrypted:	false
SSDEEP:	3072:jBNmLqpxDPt+pt1VPA9TRtQuTqLWe5fJZhuCQm+1yUVNSmE:tm0yt1VP0guTqFJSbmJUSt

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_2.txt	
MD5:	68BC76A5DF7A7C5368E8AC9484584825
SHA1:	8523D1CD6709B58F7ACE6EE6F08343DF6BFFDBDF
SHA-256:	E5171BF897A4D8C420708E09D1DB070A185EBAC7010E17AE7695541C383A95DB
SHA-512:	C2320BEE41FFD37CB945AC131578A3F873B4BB5FD6D46BBA6DCEFD061946E3359F7F95D4DB5FA18C20E8DB602AFC8D53824D18AFA6643AAA58A9B2BD2D8C81EE
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....“0..C^.C^.C^....C^.....C^..%.C^.C_..C^....C^....C^....C^....C^.Rich.C^.....PE..L...?v^.....X.....@.....Z.....0...J.....d....X.....@Z..... .....?..@.....text...z..... ..`.data...P.V.....N.....@....rsrc.....X.....@..@.reloc...I...@Z..J.....@..B.....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_3.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	625152
Entropy (8bit):	7.547054954032131
Encrypted:	false
SSDEEP:	12288:mjTb2XoEiL2HWXI7xfyhrIMdaQ6mgJ5mpaeyRfo:OTb9SKOfqV4Q/g3mpad
MD5:	208EF3505E28717F9227377DA516C109
SHA1:	FE9D2E9A69268EE0D98A29013F5E6123A0A09C32
SHA-256:	52F5B95AB8E5791BE49A321279D65D57FD65753167ABDD94DD705E3998229570
SHA-512:	C5AC3FB177367E9CE5C7BD1598558BA1D1CE63E517DF2EA92A86D1ED320A3449EE945ACC456CB92816BB76DE206F2583E7659FF9D15A007E0347010181B477D
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....“0..C^.C^.C^....C^.....C^..%.C^.C_..C^....C^....C^....C^....C^.Rich.C^.....PE..L...#.N^.....\....X.....G.....p....@.....@`.....M.....j..F...._..d....`^.....,_.... .....?..@.....text....Z.....\..... ..`.data...P.V..p...N..`.....@....rsrc.....`^.....@..@.reloc..:M...._..N...<.....@..B.....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_3.txt	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	625152
Entropy (8bit):	7.547054954032131
Encrypted:	false
SSDEEP:	12288:mjTb2XoEiL2HWXI7xfyhrIMdaQ6mgJ5mpaeyRfo:OTb9SKOfqV4Q/g3mpad
MD5:	208EF3505E28717F9227377DA516C109
SHA1:	FE9D2E9A69268EE0D98A29013F5E6123A0A09C32
SHA-256:	52F5B95AB8E5791BE49A321279D65D57FD65753167ABDD94DD705E3998229570
SHA-512:	C5AC3FB177367E9CE5C7BD1598558BA1D1CE63E517DF2EA92A86D1ED320A3449EE945ACC456CB92816BB76DE206F2583E7659FF9D15A007E0347010181B477D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....“0..C^.C^.C^....C^.....C^..%.C^.C_..C^....C^....C^....C^....C^.Rich.C^.....PE..L...#.N^.....\....X.....G.....p....@.....@`.....M.....j..F...._..d....`^.....,_.... .....?..@.....text....Z.....\..... ..`.data...P.V..p...N..`.....@....rsrc.....`^.....@..@.reloc..:M...._..N...<.....@..B.....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_4.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.697202721530063
Encrypted:	false
SSDEEP:	96:CyJOuTNNLXqqCWV2sLZS4kdtKozt15BHf7BKEzNt:C0Tj2qH39Gt35BHsu
MD5:	DBC3E1E93FE6F9E1806448CD19E703F7
SHA1:	061119A118197CA93F69045ABD657AA3627FC2C5

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_4.exe (copy)	
SHA-256:	9717F526BF9C56A5D06CCD0FB71EEF0579D26B7100D01665B76D8FDD211B48BD
SHA-512:	BEAB2F861168AF6F6761E216CB86527E90C92EFC8466D8F07544DE94659013A704FFEAA77B09054F2567856C69DF02434DE7206A81A502B738D14D8F36F0DA84
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....4... ...@....@.. ..... ..@.....4..W....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....4.....H.....L$..H.....0.....~....,(.....,(....~....,(.....,(....~....,(.....,(....~....,~.... ... .Z(....~....,r...pr...p.(....&r...p(.....(....r...p(.....(.....(...~....&*...0..q..... ....(.....(....t.....r...po....o....t.....o.....s.....o.....o.....o.....o.....,.o....& ....(.....*.....:..W.....aa. .....0.....(....o....r...p(.....(.....(...-.(!...o".....(

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_4.txt	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.697202721530063
Encrypted:	false
SSDEEP:	96:CyJOuTNNLXqqCWV2sLZS4kdtKozt15BHf7BKEzNt:C0Tj2qH39Gt35BHsu
MD5:	DBC3E1E93FE6F9E1806448CD19E703F7
SHA1:	061119A118197CA93F69045ABD657AA3627FC2C5
SHA-256:	9717F526BF9C56A5D06CCD0FB71EEF0579D26B7100D01665B76D8FDD211B48BD
SHA-512:	BEAB2F861168AF6F6761E216CB86527E90C92EFC8466D8F07544DE94659013A704FFEAA77B09054F2567856C69DF02434DE7206A81A502B738D14D8F36F0DA84
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\7zS4FBAB23D\arnatic_4.txt, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....4... ...@....@.. ..... ..@.....4..W....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....4.....H.....L$..H.....0.....~....,(.....,(....~....,(.....,(....~....,(.....,(....~....,~.... ... .Z(....~....,r...pr...p.(....&r...p(.....(....r...p(.....(.....(...~....&*...0..q..... ....(.....(....t.....r...po....o....t.....o.....s.....o.....o.....o.....o.....,.o....& ....(.....*.....:..W.....aa. .....0.....(....o....r...p(.....(.....(...-.(!...o".....(

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	860160
Entropy (8bit):	6.627703871145996
Encrypted:	false
SSDEEP:	24576:/kRkLis0EC5vKcYE52sYAt2rKzTmExr8:570nFNYwzTLxr8
MD5:	4A1A271C67B98C9CFC4C6EFA7411B1DD
SHA1:	E2325CB6F55D5FEA29CE0D31CAD487F2B4E6F891
SHA-256:	3C33E130FFC0A583909982F29C38BFFB518AE0FD0EF7397855906BEEF3CD993D
SHA-512:	E9FC716C03A5F8A327AC1E68336ED0901864B9629DCFD0A32EFE406CDFC571C1BD01012AA373D2AD993D9AE4820044963A1F4CD2BA7EBE5A4B53B143B7B7A2C2
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....v0..c..c..c...b..c...bf..c...b..c...b..cV:.c..c...b[..c...b..c...b..c...b..c..cm ..c...b..c...c..c..c..c...b..cRich..c.....PE..L....n.`.....m.....@.....`.....@.....P....0.....I...>..8..... .....x?.....>..@.....text..... ..`.rdata.....@..@.data....o.....L.....@....rsrc.....0.....@..@. reloc...l.....n.....@..B..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.txt	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	860160
Entropy (8bit):	6.627703871145996
Encrypted:	false
SSDEEP:	24576:/kRkLis0EC5vKcYE52sYAt2rKzTmExr8:570nFNYwzTLxr8
MD5:	4A1A271C67B98C9CFC4C6EFA7411B1DD
SHA1:	E2325CB6F55D5FEA29CE0D31CAD487F2B4E6F891
SHA-256:	3C33E130FFC0A583909982F29C38BFFB518AE0FD0EF7397855906BEEF3CD993D

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.txt	
SHA-512:	E9FC716C03A5F8A327AC1E68336ED0901864B9629DCFD0A32EFE406CDFC571C1BD01012AA373D2AD993D9AE4820044963A1F4CD2BA7EBE5A4B53B143B7B7A2C2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....v0..c..c..c...b..c...bf..c...b..c...b..cV:.c..c...b[..c...b..c...b..c...b..c..cm ..c...b..c...c..c..c...b..cRich..c.....PE..L....n.`.....m.....@.....`.....@.....P....0.....I...>..8..... .....x?.....>..@.....text..... ..`.rdata.....@..@.data....o.....L.....@....rsrc.....0.....@..@. reloc...I.....n.....@..B..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_6.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	168960
Entropy (8bit):	5.751236745493968
Encrypted:	false
SSDEEP:	3072:0F8DeftClWsgBZf98dmu5tcyNH+gL/GxS:E8QCQsIf9Y5SSnG
MD5:	08E6EA0E270732E402A66E8B54EACFC6
SHA1:	2D64B8331E641CA0CE3BDE443860CA501B425614
SHA-256:	808791E690E48577E7F43B9AA055FA0EFB928EF626B48F48E95D6D73C5F06F65
SHA-512:	917554CA163436F4F101188690F34A5AB9DD0CFD99CD566830423B3D67FA1DA3E40F53B388D190FEF9EB3F78B634D3C72330E545219DE7570939A9539F5950F9
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R..`.....".....I...$.....@.. ....@.. ..... ..... ..@.....G..S.....@..H.....!.AHg.#. .... .....@....text....i...@...j..... ..`.rsr c.....@..@.reloc.....@..B..... ..`..... ....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_6.txt	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	168960
Entropy (8bit):	5.751236745493968
Encrypted:	false
SSDEEP:	3072:0F8DeftClWsgBZf98dmu5tcyNH+gL/GxS:E8QCQsIf9Y5SSnG
MD5:	08E6EA0E270732E402A66E8B54EACFC6
SHA1:	2D64B8331E641CA0CE3BDE443860CA501B425614
SHA-256:	808791E690E48577E7F43B9AA055FA0EFB928EF626B48F48E95D6D73C5F06F65
SHA-512:	917554CA163436F4F101188690F34A5AB9DD0CFD99CD566830423B3D67FA1DA3E40F53B388D190FEF9EB3F78B634D3C72330E545219DE7570939A9539F5950F9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R..`.....".....I...$.....@.. ....@.. ..... ..... ..@.....G..S.....@..H.....!.AHg.#. .... .....@....text....i...@...j..... ..`.rsr c.....@..@.reloc.....@..B..... ..`..... ....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_7.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	157696
Entropy (8bit):	5.817263024080333
Encrypted:	false
SSDEEP:	3072:vz8qB8b+YWRzy5T9Ixj2Q5C2APy1LofKkcf1JcwQe9uJ21tKDW6:vz8Tb+JRzy5TYjB0PPy1LaXM16k9uk1o
MD5:	614B53C6D85985DA3A5C895309AC8C16
SHA1:	23CF36C21C7FC55CAB20D8ECB014F7CCB23D9F5F
SHA-256:	C3818839FAC5DAFF7ACD214B1CA8BFDFA6CE25D64123213509C104E38070F3F9
SHA-512:	440361B70C27EE09A44D8D734E5ABD3C2C2654EA749FD80A8CBADD06A72313284468F9485DAB0CFF0068F7F3325A78442E36E0EC8E110D70F04746736BF220C
Malicious:	false

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_7.exe (copy)	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.....V...V...VE..V...VE.*V...V..fV...V...Vp..VE..V6..V..vV...V.;.V...V. ..V...V.;+V...VRich...V.....PE..d.....g].....#.....`.....^.....@..... .....p...?...P.....h.....s..8.... .....p.....p..P.....text....^.....`..... ..`.rdata.....p.....d.....@..@.data....?.....@....pdata.....P.....@..@ .rsrc....?...p...@...(.....@..@..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_7.txt	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	157696
Entropy (8bit):	5.817263024080333
Encrypted:	false
SSDEEP:	3072:vz8qB8b+YWRzy5T9Ixj2Q5C2APy1LofKkcf1JcwQe9uJ21tKDW6:vz8Tb+JRzy5TYjB0PPy1LaXM16k9uk1o
MD5:	614B53C6D85985DA3A5C895309AC8C16
SHA1:	23CF36C21C7FC55CAB20D8ECB014F7CCB23D9F5F
SHA-256:	C3818839FAC5DAFF7ACD214B1CA8BFDFA6CE25D64123213509C104E38070F3F9
SHA-512:	440361B70C27EE09A44D8D734E5ABD3C2C2654EA749FD80A8CBADD06A72313284468F9485DAB0CFF0068F7F3325A78442E36E0EC8E110D70F04746736BF220C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.....V...V...VE..V...VE.*V...V..fV...V...Vp..VE..V6..V..vV...V.;.V...V. ..V...V.;+V...VRich...V.....PE..d.....g].....#.....`.....^.....@..... .....p...?...P.....h.....s..8.... .....p.....p..P.....text....^.....`..... ..`.rdata.....p.....d.....@..@.data....?.....@....pdata.....P.....@..@ .rsrc....?...p...@...(.....@..@..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_8.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	305664
Entropy (8bit):	7.190712048851076
Encrypted:	false
SSDEEP:	3072:i8vnVAwdwUW/zqBNBodkjTOuitnFRXuwI3jiJA/ErKEmPCGb0lPY5dhuCQVfzV/O:iWnVAwdwUOLrtFxhej8A8rOolbbVh09
MD5:	CFD5BF006F5EFC51046796C64A7CB609
SHA1:	3986E827277402E2E902B971D2A6899F0C093246
SHA-256:	14F4AAC647633049977B71B4CEBCE224A400B175352591D5B6267D19A9B88135
SHA-512:	77BB324E953AFA8F5E613D5E6D82410FB40F142B200CE99B28E773A0987A0FA361524863BBCF86E8640223E5BEBB3FE7B556E3EFA41E6873E1E3D8C648E84EF3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....O^.....Y.....A.....@.....P\.....J.....d....Z.....P.....`&..@..... .....text...Z..... ..`.data.....W.....J.....@....rsrc.....Z.....@..@..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_8.txt	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	305664
Entropy (8bit):	7.190712048851076
Encrypted:	false
SSDEEP:	3072:i8vnVAwdwUW/zqBNBodkjTOuitnFRXuwI3jiJA/ErKEmPCGb0lPY5dhuCQVfzV/O:iWnVAwdwUOLrtFxhej8A8rOolbbVh09
MD5:	CFD5BF006F5EFC51046796C64A7CB609
SHA1:	3986E827277402E2E902B971D2A6899F0C093246
SHA-256:	14F4AAC647633049977B71B4CEBCE224A400B175352591D5B6267D19A9B88135
SHA-512:	77BB324E953AFA8F5E613D5E6D82410FB40F142B200CE99B28E773A0987A0FA361524863BBCF86E8640223E5BEBB3FE7B556E3EFA41E6873E1E3D8C648E84EF3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_8.txt	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....O^.....Y.....A.....@.....P\.....J.....d....Z.....P.....`&..@..... .....text...Z..... ..`.data.....W.....J.....@....rsrc.....Z.....@..@..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\libcurl.dll	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	223232
Entropy (8bit):	7.91725038805347
Encrypted:	false
SSDEEP:	6144:Kk3jgivfCVSRrLV7yAVzKZIjCbanUKWw+ba//PXHUo:30iH0iVPVzKOOunLWf2//0
MD5:	D09BE1F47FD6B827C81A4812B4F7296F
SHA1:	028AE3596C0790E6D7F9F2F3C8E9591527D267F7
SHA-256:	0DE53E7BE51789ADAEC5294346220B20F793E7F8D153A3C110A92D658760697E
SHA-512:	857F44A1383C29208509B8F1164B6438D750D5BB4419ADD7626986333433E67A0D1211EC240CE9472F30A1F32B16C8097ACEBA4B2255641B3D8928F94237F595
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J4e`....Y.....!.....Dk..... ..... .....-... ...<.....text.....t.....`.P..data.... .....z.....@.`..rdata..... ...F.....@.`./4.....4.....@.0..bss....h.....`..edata.....@.0..idata... .....@.0..CRT.....@.0..tls .....@.0..rsrc.....@.0..reloc...@.....&.....@.0./14.....P.....8.....@.@./29..... ...`.....:.....@.../41.....J..... ..@.../55.....L.....@.../67.....N..

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\libcurlpp.dll	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55808
Entropy (8bit):	6.9891040161841085
Encrypted:	false
SSDEEP:	768:W//WT2mbP+7x4Mx5KzVAn/QqvtdZs8LlR67diTNh4joK7qmQhyOl4UuGoxX9j3D:WHIK1R2VA/Qqvtzz67dbn1QhyOl4UuD
MD5:	E6E578373C2E416289A8DA55F1DC5E8E
SHA1:	B601A229B66EC3D19C2369B36216C6F6EB1C063E
SHA-256:	43E86D650A68F1F91FA2F4375AFF2720E934AA78FA3D33E06363122BF5A9535F
SHA-512:	9DF6A8C418113A77051F6CB02745AD48C521C13CDADB85E0E37F79E29041464C8C7D7BA8C558FDD877035EB8475B6F93E7FC62B38504DDFE696A61480CABAC 9
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Gf`....B.....!.....T.....0.....(k.....`.....x... ....0F.. @..$.....DA.....?.....text.....4.....`.P..data.....:.....@.0..rda ta.....<.....@.`./4.....@.....B.....@.0..bss.....`..edata...P... ...H...R.....@.0..idata... ...p.....@.0..CRT..... ..@.0..tls.....@.0..reloc.....@.0./14.....@.@./29..... .....@.../41.....@.../55..... .....@.../67.....@.0./80..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\libgcc_s_dw2-1.dll	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	116238
Entropy (8bit):	6.249236557413483
Encrypted:	false
SSDEEP:	3072:nti6N0WeF35Ro7hAWP6cagLSuf6LG3qSbKE4M:ti6N2F33wGJVuHuE
MD5:	9AEC524B616618B0D3D00B27B6F51DA1
SHA1:	64264300801A353DB324D11738FFED876550E1D3
SHA-256:	59A466F77584438FC3ABC0F43EDC0FC99D41851726827A008841F05CFE12DA7E
SHA-512:	0648A26940E8F4AAD73B05AD53E43316DD688E5D55E293CCE88267B2B8744412BE2E0D507DADAD830776BF715BCD819F00F5D1F7AC1C5F1C4F682FB7457A20 0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#....^.....p....n.....0..... .....u..... ..$.....D.....text....\.....^.....`.P`.data...,....p.....b.....@.0..rdata..T..... .....d.....@.`@/4.....4.....4...r.....@.0@.bss.....`..edata..u.....@.0@.idata.....@.0..CRT....,..... ..@.0..tls.....@.0..reloc..$.... .....@.0B..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\libstdc++-6.dll	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	662528
Entropy (8bit):	7.222450867745387
Encrypted:	false
SSDEEP:	12288:ZGRoW1chMjnv+gvJhb6bmpPSmCnh4o0v4Mc2jTrKoDSwq/3PmkfT4CmwcMcP1uE:uowcmBhKmlC4o0v4k1
MD5:	5E279950775BAAE5FEA04D2CC4526BCC
SHA1:	8AEF1E10031C3629512C43DD8B0B5D9060878453
SHA-256:	97DE47068327BB822B33C7106F9CBB489480901A6749513EF5C31D229DCACA87
SHA-512:	666325E9ED71DA4955058AEA31B91E2E848BE43211E511865F393B7F537C208C6B31C182F7D728C2704E9FC87E7D1BE3F98F5FEE4D34F11C56764E1C599AFD02
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#.....H.....0.....`.....o.....`..... .....w.. @..$.....DA.....?.....text....P.....B.....`.P..data.... ..`.....F.....@.`..rdata..... ..>...H.....@.`./4.....`.....@.0..bss.....`..edata.....x...6.....@.0..idata... ...p.....@.0..CRT.....@.0..tls. .....@.0..reloc.....P.....@.0..aspack.. ...0.....`....adata.....P.....@..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\libwinpthread-1.dll	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	70656
Entropy (8bit):	6.292322392729986
Encrypted:	false
SSDEEP:	1536:xPCESXKWzkxTz8uLfdkWr2sUX8YNKykl1wwwwUXrMZE4cYdz:x6baWwxH8EzSHYZE4cYdz
MD5:	1E0D62C34FF2E649EBC5C372065732EE
SHA1:	FCFAA36BA456159B26140A43E80FBD7E9D9AF2DE
SHA-256:	509CB1D1443B623A02562AC760BCED540E327C65157FFA938A22F75E38155723
SHA-512:	3653F8ED8AD3476632F731A3E76C6AAE97898E4BF14F70007C93E53BC443906835BE29F861C4A123DB5B11E0F3DD5013B2B3833469A062060825DF9EE708DC61
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....,Q.....#.....@.....d..... ....@.,.....p..P.....(.....`.....A..d.....text.....`.P`.data.....@.0..rdata..... .....@.`@.bss.....`..edata..,.... .....@.0@.idata..,....@.....@.0..CRT....0....P.....@.0..tls.... ....`..... .@.0..rsrc...P....p.....@.0..reloc..(.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe	
Process:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	297472
Entropy (8bit):	7.956679998165027
Encrypted:	false
SSDEEP:	6144:SCqbkrMCqbFE9VFvRrEQWjinXABNAPWYC2cFDdo:S4rQBEZ5MiXAkPWYhc5d
MD5:	774F0D5B7DC3D2AD9CC4A0D921C9DA8B
SHA1:	74B7AA0A726BEEE6708A1164D1C7EB3E3CE687CE
SHA-256:	29C4D520A083C1707FDC769E0FF9E936372F54294A85F671F24FE4C8FFA937D3
SHA-512:	57BEE412C206AA0FEA2D72130EE7B71BF933778A2D0C49D4314EE44C98350D581882EF7BBF4051E28B75ED0FB09A454FFB83203AAC4ABC49C5831E141B70076
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`....\Y.....H.....@.....I..... ..... ...p.....text.....`.P..data.... .....@.`..rdata..... .....@.`./4.....@.0..bss.....`.....`..idata.....p.....@.0..CRT.....@.0..tls.....@.0./14..... .....@.@./29.....@.../41..... ...@.....@.../55.....`...`...$.....@.../67.....@.....@.0./80.....B.....@.../91..... .....D.....@.../102..... .....r..

C:\Users\user\AppData\Local\Temp\CC4F.tmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_2.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1622408
Entropy (8bit):	6.298350783524153

C:\Users\user\AppData\Local\Temp\CC4F.tmp	
Encrypted:	false
SSDEEP:	24576:hNZ04UyDzGrVh8xsPCw3/dzcldJndozS35IW1q/kNVSYVEs4j13HLHGJImdV4q:dGrVr3hclvnqzS35IWk/LvRHb0
MD5:	BFA689ECA05147AFD466359DD4A144A3
SHA1:	B3474BE2B836567420F8DC96512AA303F31C8AFC
SHA-256:	B78463B94388FDDB34C03F5DDDD5D542E05CDED6D4E38C6A3588EC2C90F0070B
SHA-512:	8F09781FD585A6DFB8BBC34B9F153B414478B44B28D80A8B0BDC3BED687F3ADAB9E60F08CCEC5D5A3FD916E3091C845F9D96603749490B1F7001430408F711D
Malicious:	false
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\Documents\23BwEXBCcNvhGv9NYNw8QgCc.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:CwjqfkkAdjbngxNmJEVYhGEZUMTQFNWY9ANrtjIUhzl4rCLowo9K60eccwzscsgx:wfyjbngcEOHUMUF4YO70405RnYcl
MD5:	FC34A4518C3721FF250AC962733C8461
SHA1:	0228DE93D9EF77FCFF9ECB02659828BA67F40117
SHA-256:	EC3CCB5F1B8278ED67B5764B45E3A0BE586A77A6FF3C8064BA660360F8023CB8
SHA-512:	3957C52B795024A606DFAE61DCD032929BFC25C8103AAA387C7866F19DBD606C8891377F66243EC536D4E5D6B5C5C606C80355962BB548482455C6C1E1C7D60
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L...[2.`.....v.....@.....P.....0.....P.....@..... .....L.....text..... ..`.data.....@....vubi.....@....runutu.....@....tih.....@....rsrc.. .0.....@..@.reloc...J...P...L...^.....@..B..... .....

C:\Users\user\Documents\2YlsoBLp3EMqm7duutiwa6KD.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7KLcXaoD:J0+oxBeRmR9etdzRxGezH0q72ma+
MD5:	C8DDCE4DE7D2FD26927E6DB3D554AFD0
SHA1:	4C3F77BB7CD753C5F9DB1B780DF00E14D49BB618
SHA-256:	4A47941324BC9F45254B507AA228D2652064B7277C7FCB0674D1E5FE7DC68467
SHA-512:	FB2A5C27B410449BAA3BF9142A38862337E37FD21712AD21C7CDBF3DDBAB76AE4A6153D756B61DB23D9F931D300333BA6B87319F8955E7EEB401D306BC346C2 8
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.45 Port 80</address>.</body></html>.

C:\Users\user\Documents\3afsq2MGMno51lOXdmeStaLk.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:mP98+Pmw4Jl/gzq4R+dWgEQ5YX8li//Hvil1:meomw47gzEdWgrbk//HU
MD5:	652CE60F8D1EA7AC21DAC40073AF2321
SHA1:	2C602E0D76C208DF0F9A305E3D6502BCCB8FF073
SHA-256:	BDA915D15E254F51EEA3F691857DB7E6E35443F4F29C5EE258E4D03127F180BE
SHA-512:	DCED8F2CFA741840EDB018B36A638CD229588A9AF985DBF7BAC38B8F7F8682AE721DB0639FAC163594CCFCFC7DA37DE4FF79D25B6D100B1F01D7E39F4E2B1 C2

C:\Users\user\Documents\3afsq2MGMno51lOXdmeStaLk.exe	
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....Y.....0.....H..... ... .@.....w....@.....0.....@...E..... ..ctors... .....`.adata.....0.....@....rsrc....E...@...E.....@..@.bss.....y...L.....@..... .....\m..w.-4}U#4_em.p`QG*...8.. {.k

C:\Users\user\Documents\43mXpM5vSV6ag5hl43kJE3nj.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:f9oCDm4QZLyLB2dFFMwbIUOTPZyZSZ2eCAGlfMy3iyK+hGvXKW4BvCuk:rb8PMwbIVMZSZ1cMB16lsz
MD5:	67848A34646ADF30BCC92518C0AE1BD1
SHA1:	CD098705414B24EB5AB2D1DAA2E42A365AB332DE
SHA-256:	DFD81F4D4795EE535C2D6166C9226F5EF440E696EB572105329A73A704787AA3
SHA-512:	EE98CEDDA9ADF054A8C8EB5ADC6CC2073E39FAD599A6CE92EEE151F896AF6EFFD19E66D89EDFBF352E0BA47B8E48BC34F6AF56225E9AED5AC7DA86D2A62E71D2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L.....`_.....@.....P|.....Z.....(.....|.....0...@.....D..... .text...D..... ..`.data.....@....dohayi.....@....vapocav.....@....nivepo.....@....rsrc.....`_..... .....@..@.reloc...J....|..L.....@..B..... .....

C:\Users\user\Documents\4kmOewH8kDodZZ2lCCJUwR4o.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3072:CwM8ll/9+Qa/PHsuH3EbSSSSSabsZGpu:9nQQQacuqSSSSSabsZG
MD5:	A9DED7D6470F741B9F4509863665F74C
SHA1:	FF1A2ABB33D9DD290C9349565586C6C1E445DC1E
SHA-256:	2F326116DF411C1C9AA3728E0C191FD0888FF63DB7DB08CC70DB1F1AEBE88347
SHA-512:	507D729DDC2533616A6DF372BB8C175D44DC5B68D0A455496DE34019FCF685A6EF6A36693CCB9417637CB9783CFD48EDB039274A7C51476FD39F98796B1D78D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.....0..... ....@.. .....N.. ..@.....S.... .....H.....`_...&.tJ... ...L.....@....text...`.....P..... ..`.rsrc..... .....@..@.reloc.....@..B..... ..` .....

C:\Users\user\Documents\5VYY5Jfm1TgW9nVctu3WNDWJ.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7gLcXaoD:J0+oxBeRmR9etdzRxGezH0q7gLma+
MD5:	978489E2DDB94E1A8F3C4842596BED8B
SHA1:	CCDAA1B6E674D7D7F6E2FE7233239ADD9D62CC75
SHA-256:	222FF59C7DCD2FFE6BBFAA15DDA759C48F5F205DF0B82BCF969FAF845C1F12E2
SHA-512:	A99B30607BF0FD80458374DE3688C7E1AE5FF2CEDE946DA308B13BA5639B0500E69A09E2B8A94BEDB0D59B4B5B031149AFEE6E98C2556254EFFC1A6D8EECE837
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.29 Port 80</address>.</body></html>.

C:\Users\user\Documents\62ZxL2NI48wEtSDqLisV5B5p.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:flSQc2qhAGg2AV5c+dznE1rA8r6nDDrBC14SrxCbsxg7GMjH5oRWSe:f4Qc2BG0cunERAtBC1Pd8sxSbZoRW
MD5:	D08898F15B9373D16001E84A320628E5
SHA1:	9350EC1E0FCA1C3E78A56025596D4A230832BBBE
SHA-256:	018AE123C7095FA1CF54A2FED5F54A4E953A556BB1B180D80E9D955351A93DB8
SHA-512:	A66929317B32590312BF81CF64EC2F89524159C28AB86E40095EBEA41267E78C61C716BA73183DB82991C5C55D6C4002E845C24DAE92EFFF2BD0D2FE3BECE00
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I..U(...(...(...6.).1...6.?.W....I..+...(.....6.8.....6.(.)...6.-.)...Rich(..... .....PE..L....fe_.....X...v.....6.....p....@.....Q.....S..(....@...{.....X.....@.....8..... .....text...HW.....X..... ..`.data.....p.....\.....@....mepav.....t.....@....butoji..... .....v.....@....xuteru.....0.....x.....@....rsrc.... {...@...|.....@..@.reloc...F.....H.....@..B..... .....

C:\Users\user\Documents\AVKqP7CFw2sgxjPkEFXixv3V.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	196608:91OLi0Xz1oNNxRqT8kMmyur5ums3v2DF2r:3Oe0D2Txw8Hmd5uxvF
MD5:	F7A84C588542DBD6AAB35892B9D88DCD
SHA1:	531ED1D8622968E1979D2561D5F98ADBAEC40B31
SHA-256:	DBF97E84632CCD62E28F0A7CC717A5C5C67D9FF99638D8D12084DC6796761E04
SHA-512:	7C2EED1DA4E18605D8B3B85A71079B2084586F2C0F013283F9CFF3A0B0D94595550C8BE0DA2DB6D6B38A6E56498895842FE14F8E6F78B809C9591FB27073E1D6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..s...s...s...}...s...y..s...,...s...r.!.s.....s...x..s.....s.....s.^.u. ..s.Rich..s.....PE..L....S.L.....K.....@.....d....p..`..... .....text.....  ..`.rdata...D.....F.....@..@.data...HZ.....2.....@....sxdata.....`.....@....rsrc...`....p.....@..@..... ....

C:\Users\user\Documents\E720L1M1wcDP03pvh4WlMQD6.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:b/D0I7bieAtJl4gcl4LxzuB5IK+hJEacXVeN19xPkNj:b/xAZclKxYIINFefPGj
MD5:	3ECFD5D9F991294510E111DCF96357FD
SHA1:	7B208DA6822F3B04E27F0B1DCE0E48B11D3E7DA7
SHA-256:	9F7FDE5DC8DD5812E5F58AAB39268D6FFB15FD7A1CCD77686FA970EF55693F85
SHA-512:	36DD26FB198A46E7B453BF13D781BB4F3F970368869BBCBC0F5D8472BAC22B42ABCD41705EB0A0F3085079C8CF37E18513BB695F3EA7210C8D622C630C5039C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L.....0.....H..... ...@....@.....@.....@.....`.....p..pG..... ...gfids...P.....`BSS.....`.....@....rsrc...pG...p.....@..@BSS.....y...$.....@..... .....on..D.}[A.y[[C%.x..t.k..i...

C:\Users\user\Documents\KZb7b5nQhyxywttU5a6OGhmR.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\Documents\KZb7b5nQhyxywttU5a6OGhmR.exe	
SSDEEP:	12:TjeRHdHiHZdtkll5r4NGlTF5TF5TF5TF5TF5TFK:neRH988aTPTPTPTPTPTc
MD5:	9E47D3A502A7B2BCEC1F1375430CA0EB
SHA1:	E3845E5E982AE0580FA31ABF301C803D89ADAB52
SHA-256:	CBF1FDFDB7257DAF8B0905D94BD04E2829C502C9C01B1D96BB979069E2EBC895
SHA-512:	8239210B404E0B19E841D7832D73452617A17C39A29F7CB6E8CCE8F1474B7C17D6ACBA630EFB6510CB3F0315C3147B7BB62C0B0BEECEF8EF29764B8B906E8EF3
Malicious:	false
Reputation:	unknown
Preview:	<html>..<head><title>404 Not Found</title></head>..<body bgcolor="white">.. 404 Not Found ..<hr> nginx/1.14.0 (Ubuntu) .. </body>..</html>.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->..

C:\Users\user\Documents\LGWvGO5nGkFCrd4L2uFL5DeK.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:CLw0gZFUJuzEpCMQaVQ3luptUH2jQ66PYTnxRcqh+ZygmiuLscbTzAIIbasU+By:mPJOqppLUHWP6PY7xRUjAocF+Fn
MD5:	399A7496E00DAC0E986FB7E4842E6A2C
SHA1:	8C837A80329CD1894050AE8163881289A971A99E
SHA-256:	7747F0397EF330B53D0BD68DFE9ED416A935851760657B7DF0ED93A7A8A5692C
SHA-512:	75B3467BC465E7AC9841E6A742A21373F2A044C0266C388B7BB63331ACEE73E05EAA329E4B3A700FF1EEF0C85D84F128D72D119B5018A1B29C88E29B8589D8E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....>.... .....@.. .... @.....W..... ....H.....text...D.... ....`.rsrc.....@..@.reloc..... .....@..B..... .....H.....$7.....PD.....t.....g.....y....(.E..*.s.?...W...**....(i...*f....(j...r7..p(....(k...*f....ol...(m...ol...on...*.sCD...\| ...*f....ol...r.#.p(....on...*f....o....r.#.p(....on...*f....o....rO$.p(....(k...*.....o....r.$.p(....r...p(....r-..p(....(....on...*f....o....r4%.p(....(k...*f....o....rv%.p(....(k...*f....o....r.&.p(....(k...*f....o... .rk&.p(....(k...*.~....:#...r.&.p(.....#...(....o....s.....~....*.~....*.~

C:\Users\user\Documents\MBQu1S3moACEXZ87D1YEJhpQ.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7KLcXaoD:J0+oxBeRmR9etdzRxGezH0q72ma+
MD5:	C8DDCE4DE7D2FD26927E6DB3D554AFD0
SHA1:	4C3F77BB7CD753C5F9DB1B780DF00E14D49BB618
SHA-256:	4A47941324BC9F45254B507AA228D2652064B7277C7FCB0674D1E5FE7DC68467
SHA-512:	FB2A5C27B410449BAA3BF9142A38862337E37FD21712AD21C7CDBF3DDBAB76AE4A6153D756B61DB23D9F931D300333BA6B87319F8955E7EEB401D306BC346C28
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.45 Port 80</address>.</body></html>.

C:\Users\user\Documents\PYTMx3vXyW318zqGAUpoVhbY.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:E8f39B+OecSnrJYG4oPSiANTfUrnmXb9mL8VkFq5aXq5Uzr0W:porJYGPyTenmZ64+3zr9
MD5:	BF577170C86E15B04BA705FD3F07151F
SHA1:	2647B6F5968B8521FC3A024E3600554D8746A4D8
SHA-256:	901CA296CF9AAA112CA787FAE18AB87AE5E8DAF1ECB037F0A2BEA44F9125E8DA
SHA-512:	CD04DC5243444953F08BA159800315DE9636C08BEE1814D53E711440799E6EAF277337EE0021C7076AA47084C4203B7196CADEC38FA75C35EE01F20875138EF0
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\PYTMx3vXyW318zqGAUpoVhbY.exe	
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.........+..R...d:.....Q..... ....PE..L....j.....0..<..... ...`....@.....  .....@.....@..... ..didata..p.....`.pdata.....@....rsrc...@.....@.....@..@.text.....Ax.....@..... .....G..sl.0.gmY.=.'....mL.{.

C:\Users\user\Documents\R2IpdvMDW3mqJjP0F3OqthCG.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:NPfr7cLGO+vNNeB/b39qxwL9AtxansJWBpB2Ol1acxTWwnWQL:Nr7cLGvIB/ExPxPcjBrl19TW9a
MD5:	5BF9D56B1B42412A2B169F3FB41B2A4D
SHA1:	E52BA18C693843BB1A72FCA134AFBDE40A0568DF
SHA-256:	02D1BCDDD657EC1F5C83A8420E6C30FC2A83980FFCC05A0C3BB9CFA70ED1FA06
SHA-512:	E87CA5E5F7CBEF70A275C1294C3E9FC27B35A370C01F17CA84E22C99381BD96E7DDC89748D6A12D069B013E93FE2C60FA810EC98C6C4EEC864E8D1B2EF0EF1F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W.7,..(~W.Rich)~W.....PE..L..#:._.....k.....@.....P.....(.....@.....@..... .....L.....text..... ..`.data.....@....nan.....@....dis.....@....fubah.....@....rsrc... (.....@..@.reloc..hG...@...H...T.....@..B.....

C:\Users\user\Documents\RcGzT5XRuDFwXklj8ZcXjhgH.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	49152:7rEOLD0xW+aJVXfxu3Eosp/qw7RV+uY/:023Jtosp/qw7yb
MD5:	DD3C57E2520A47D634E5FAAC52782FDA
SHA1:	73AF831AA23F72D82FE80E84B0C4411E6A9DCCB6
SHA-256:	03B887397102E717DE5EF8A0D4D0374BDF5347A85DDDC8C829714770142B8FDF
SHA-512:	37F0BE02B923B873DAA2CB98A49C42A1AB2DCB3B9A5422E7B5FECFEDF1A90CE2F00E375A41C1C0331A4B3E3B96B5FBDC267907966AA8406DED1970B42F3E62C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: C:\Users\user\Documents\RcGzT5XRuDFwXklj8ZcXjhgH.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\Documents\RcGzT5XRuDFwXklj8ZcXjhgH.exe, Author: Joe Security
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....i..-..A-..A-..A9..@8..A9..@ ..A9..@...A...@...A...@,..A...@=.. A...@'..A...@...A9..@$..A-..A..A...@%..A...A,..A-.pA,..A...@,..ARich-..A.....PE..d.....a.....".....}.....@..... !.....`..... .....DJ..d.....J.....`..... ..#.. :..p.....;..(....:..0.....8.....text..... ..`.rdata...[.....\.....@..@.data.....`...^.. .N.....@....pdata..`.....@..@_RDATA.....4.....@..@.rsrc....J.....L...6.....@..@.reloc...#.... ..$.... .....@..B.....

C:\Users\user\Documents\TQad1aZzvVYenk6sBK78SpeO.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7KLcXaoD:J0+oxBeRmR9etdzRxGezH0q72ma+
MD5:	C8DDCE4DE7D2FD26927E6DB3D554AFD0
SHA1:	4C3F77BB7CD753C5F9DB1B780DF00E14D49BB618
SHA-256:	4A47941324BC9F45254B507AA228D2652064B7277C7FCB0674D1E5FE7DC68467
SHA-512:	FB2A5C27B410449BAA3BF9142A38862337E37FD21712AD21C7CDBF3DDBAB76AE4A6153D756B61DB23D9F931D300333BA6B87319F8955E7EEB401D306BC346C28
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\TQad1aZzvVYenk6sBK78SpeO.exe	
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.45 Port 80</address>.</body></html>.

C:\Users\user\Documents\WN7mKI9_SQ4ujDwH_kKQHbe7.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:HCA2YLo85KNa/jA6p8MIQfJFDrJoYkLLTE:HX2ImN4F2MTJFBoY04
MD5:	913FC52D517A4B4B2BE78103184EF87E
SHA1:	5ECF0E1AF77F229C46F13B9C4FB6341761ECD818
SHA-256:	734D3D7D77B4FAD43FF22B081E664D6CFEE09C67AEC8F81CFA524924CB7785FA
SHA-512:	1881476719098573F618A4FFB21EC6729E8B72A869AAE7D959EAF49DF5A085208F1DADFBA71ACC71A4FCCE5046FE2863A7C19EEBA04A36F13564059B23E60733
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.9.)~W.)~W.)~W.7,..3~W.7,..~W...,..~W.)~V..~W.7,...~W.7,..(~W .7,..(~W.Rich)~W.....PE..L..../._.....P.....@.....p.....t...P.....(.....@..... .....L.....text..... ..`.data.....@....ruceg.....@....todako.....@....godol.....@....rsrc.. .(.....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\Documents\WpPIUPf_de3qhcU6Yb86wV8v.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:8Qi3uAIKMYqN96m6UR0IrELWKlVwlpkTyL6Ka3EjiqxyNefotS10m:8Qi+PvNgHIALfGHkTVwiPk4Bm
MD5:	3A9664DAD384F41DCDC1272ED31171E0
SHA1:	D525F290DCF469F5B26654A4DB685092F8616509
SHA-256:	A85903FC9F06B4CCC4136FC573F6AFDFB6B90D555530F7259E4E8CB18616B724
SHA-512:	F7C3E6D561DF34C63E373C6CC715E1C13AB68013360F1694EEFAE6C896345ABD1135E60B5AA5D96FFD245AB7D24C9D856A7EAB58C9798D3B7B355E9DE16183 0
Malicious:	false
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....@.....@.....@.....P..... .....CODE....0..... ..`DATA....P.....@...BSS.....idata..P.....@....tls.....rdata..... .....@..P.reloc.....@..P.rsrc.....@..P.....@.....@..P..... .....

C:\Users\user\Documents_1UKif43Unz1FihnGsnEeFb1.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	49152:ff8wvFHfR1mO4Tkjt2iMYBYCCaYgSWRFMNbfvpxAnmWOq2gidZ6KY4i:ff8wU01BYCCabF8bXpomh1d0b4i
MD5:	C2D7BF7A4785E8B2DDC22C01C533672C
SHA1:	0302D86FC1D8A25AD147A47451BCC7D6E403F86A
SHA-256:	7322806DE0D6087D630168B501D56FBF34B00A9EA65C94A3AF51511AD3654220
SHA-512:	CE6225224E19F6FD8803267AECE0EB64D9823C3123F07783FA2F460678CC696158BF8BF78D495E33B1FFD3E2554F0E1F0F14FEFED110D7C48F0196483779A5B2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...g{.a.....$..$.....PV..Zz..`V....@..... z.....`.. .....v.Y....tz.....pz.....o..\.....uz.....fz.(.....UPX0.....PV.....UPX1.....$..`V... $.....@....rsrc.....pz.....$.....@...3.96.UPX!.$.....0E.1z...#...r.Im.....a..\..''...,J=.Q&*.d..E.. ....[aS^qm.....p$..8..`..s.&p...jMJJ...,..jDU...!..|>.....(..T(.$.~8.O...9.. (.W..orFD...o....Z6.Q.....#...,h.%.....x..y...%-y.....}.I..E....6...a*....a...5../R|..*..A.f!.&.O.K.n&.Q:.G5e<D.....+.....&...v.}x}.OL.f.....@.\.....U.k!t.....cU.l....`..\.V.X..DS.K.o.f .2p=..,Y.Y:.[.....f-lO...-a.J.A..D...F.....s.U1....c)... 6.S.].vv&.>."&.e{K.J.,.`.M]...s.u..V...S.&[..k|%<C..71.W...7..a

C:\Users\user\Documents\bCyMoheCXfvXOWdcxUFW1mSl.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe

C:\Users\user\Documents\bCyMoheCXfvXOWdcxUFW1mSl.exe	
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:Ab0yasxDZDYbVJU9Dwsn/m5eo7CKS6O4gySTePDyB9nb41xqGONesE:AYZKlUbVJeEYu9OVxePmBix/aE
MD5:	6BFC3D7F2DE4A00FAC9B4EC72520209F
SHA1:	0DC92779C7BB4C9D6C3A02FFA176199F652B3976
SHA-256:	B039B93D8CF1911397F74A703784D69363544F97F059266256CBAF419E8B2C3E
SHA-512:	DB92E098F611742A38F4B0BA5C202CE48AD926C51A6396FFEDDBC8C75891F4E104558AF7D9D108CC197BEA3CFFFDEDFFD99A9E24AD481350FA5A71DA80166 7B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#X.g9..g9..g9..yk0.v9..yk&..9..@...d9..g9..9..yk!._9..yk1.f9.. yk4.f9..Richg9.....PE..L.....L`.....2.....0O.....P....@.....-.....-..(.....~.....p.....`...@..... (.....text....0.....2..... ..`.data... ...P.....6.....@....bot.....p.....J.....@....zuxi...K.....L.....@....tive.....N.....@.. ..roduwe.....P.....@....rsrc.....^.....@..@.reloc..8;.....<.....@..B..... .....

C:\Users\user\Documents\bcqaO5hDJ96HpvV4oiEJlq3X.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	1536:a6x3MUH9LNxYEThBPnt21SnmymczorCtMqvJK2uHjmUKKDfj/RhsN:acL5T78UnmDGJuHjmUKKzrRhs
MD5:	3F13A6A1BBCEC7D68C15DEE4EEB7DF58
SHA1:	9DC2468D6E9E61D572D4C1A54B3C80DD69FF2287
SHA-256:	17D8AA92EB9BDA31A05D0BD15A52734B18AE72C9F4B6EFEF628DD5773E0F71C2
SHA-512:	E1033871C72422E80132C0E5DECE0FCBD0B9279374BC84330A3899DFFE5E94D5AFD637D45C0949D7FB775EFE07A195CB924FA9D099D2AF1A660B9A80F08807E F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Ntu.....G..-....G.....G..b...-.`.....G.....G.....G.....Ri ch.....PE..L...!._.....w.....@.....pw.....t...<.....v.....@..... .....text..... ..`.rdata..x.....@..@.data...$.s.....@....joy.....v.....@.....@..@.rsrc.....v.....L.....@..@..... .....

C:\Users\user\Documents\cgUWuTNJBuJifi7bt73hP7oj.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7KLcXaoD:J0+oxBeRmR9etdzRxGezH0q72ma+
MD5:	C8DDCE4DE7D2FD26927E6DB3D554AFD0
SHA1:	4C3F77BB7CD753C5F9DB1B780DF00E14D49BB618
SHA-256:	4A47941324BC9F45254B507AA228D2652064B7277C7FCB0674D1E5FE7DC68467
SHA-512:	FB2A5C27B410449BAA3BF9142A38862337E37FD21712AD21C7CDBF3DDBAB76AE4A6153D756B61DB23D9F931D300333BA6B87319F8955E7EEB401D306BC346C2 8
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.45 Port 80</address>.</body></html>.

C:\Users\user\Documents\duCdI76Gqz3hAbP72ldEGd_3.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3072:M1UJhFefM7JlXBTPGymqI3rfgusNKKSZrFE6dHo:vFUM7NGy2DmNvCH

C:\Users\user\Documents\duCdI76Gqz3hAbP72ldEGd_3.exe	
MD5:	7A14B5FC36A23C9FF0BAF718FAB093CB
SHA1:	DC1244688756E1E10A73C1FCBD2FCA1C3AF3565F
SHA-256:	7A1481A3EC2646610CC068CE5BBCC169D75B7B664F3DF1997823A374B1CF19A7
SHA-512:	BFE06EDB9F1928C8F7923D7FD6D3766DFF272D06F61FC4C40F1A531589D161DE435631C8B53D5D02A64AE4BEE695FB47DF6467A5B117C188813BB0CE8BE5654
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B../.qo\|.qo\|.qo\|c.l}.qo\|c.j}.qo\|c.k}.qo\|T.j}"qo\|T.k}.qo\|T.l}.qo\|c.n}.qo\|.qn\|.qo\|.qo\|.qo\|..m}.qo\|Rich.qo\|.....PE..L.....a.....r.....@.....0.....@.....$..... .....0...@.....text...7p.....r..... ..`.rdata..6`.....b...v.....@..@.data.....@....reloc..... .....@..B.....

C:\Users\user\Documents\iBq0YAwgzRU2vgFlQx44ATbt.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:4VaxLjbieAtJlVxsIkcyCqAe301sd0WwWxDY6kffDHqm:4VaIAPxscynAe30mWWwWY68bHq
MD5:	6EEAF421AA9D4768A768ECC8627D661F
SHA1:	BE3A225C182CEC3015DCCC96C6017A97C4E82CEE
SHA-256:	DCE92404D16BB8D9450234DD20AC8C3A7B8A4D3EFF019144EFBAEE25CD2BD202
SHA-512:	797868BAF5CBAD03DED67C8CA1D7ABEBF54700FEB8BD2B4A6775B27F0FD0316789254EABCD9204BB375D570B990E887CF8192F49455A6C7F9F90343483B11D4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....Q.....0.. ....@....@.....e.....@.....`.....p..H..... ...didata..P.....`.bss.....`.....@....rsrc...H....p..(.....@..@BSS.....x.....@..... .....&....2.(.V.(..x;.W.S.7.=*....

C:\Users\user\Documents\igI42Z7K7U8FCMNepiNpCeNL.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7gLcXaoD:J0+oxBeRmR9etdzRxGezH0q7gLma+
MD5:	978489E2DDB94E1A8F3C4842596BED8B
SHA1:	CCDAA1B6E674D7D7F6E2FE7233239ADD9D62CC75
SHA-256:	222FF59C7DCD2FFE6BBFAA15DDA759C48F5F205DF0B82BCF969FAF845C1F12E2
SHA-512:	A99B30607BF0FD80458374DE3688C7E1AE5FF2CEDE946DA308B13BA5639B0500E69A09E2B8A94BEDB0D59B4B5B031149AFEE6E98C2556254EFFC1A6D8EECE837
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.29 Port 80</address>.</body></html>.

C:\Users\user\Documents\l7AR_7u5i2RZzKoKItsIndOd.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:EbWxj7XagNorsFTCp64vSMLjYgrkhnuzbgwu:2Wx3a1kO6SS6c9unn
MD5:	0162C08D87055722BC49265BD5468D16
SHA1:	901D7400D1F2BC4A87EDAFD58FEBFAC4891F9FE8
SHA-256:	92F1DF4DBB0E34C38083BB9516FB5C812175B5B73C9FDA81CA8047C5C38A1ABB
SHA-512:	193A12BAF5819BC58B310BFCC5E33EEDD06C130922596A6A4F8A16BC705A28FE3D8E75C689ECFBB970F21D66FEFA7830108F661F0E95586B4D87D1DEFB85A05F
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\l7AR_7u5i2RZzKoKItslndOd.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~...-...-...-..{-...-..m-...-..j-...-.@.-...-...-...-..d-...-..z-...-...-...-Rich...-..... .....PE..L...I.`.....0....@.....@.....U.....].P....p..X.....1.....P..@.....0..... .....text...#..... ..`.rdata..b7...0...8.....@..@.data.....p.....T.....@....rsrc...X....p.....@..@..... ....

C:\Users\user\Documents\mF4pYAHQSZ4xZOo9NPmgWjXx.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	1536:nf7EzXSAH/axBSy+zotG3xKapfZVYB4gfOKKKKkcsHgcsV1JRJn2Qx:nf7EzCAHyXe0tG3ZBZVYfb5HNsV1c4
MD5:	0C70224F09C65619BC9D6AFC456294C9
SHA1:	975AA4311B2C4FEDE2DB8BD6293F5C54224348C7
SHA-256:	AC0B18AE0851CF5CB499BDCBA6BCE5D260F114768425AEED65CF6086B27A323D
SHA-512:	B72C10B8A3ED94E6E7796A562F860B9AD8F3815A3F3B9A24B98C56BD77A5318EDDCF69E41ADAD5975206C04E220107DF65BABDABF9DB98831BA567947B7936 2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e.....0..... ....@.. .....F... ..@.....S.... ..H.....H.....SH..RSn.|J... ...L.....@....text...`.....P..... ..`.rsr c...H.... .....@..@.reloc.....@..B..... ..`..... ....

C:\Users\user\Documents\oNEXKq0wVFWOWv16dlBZgDPF.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:0tRNFlFREVLL4ewt76K/lGRgOUqmq9kR6lhKX3ae/flS/riv:0HvlAVLL4e+2K/cRgOnmq9g6y5/NJ
MD5:	40D514FF4F2D184A172B988221971B80
SHA1:	F491DDE1095EFA0EE40E9A643FE3897228EE147D
SHA-256:	EE98739EFF8E6EA3B0DA03877F7D1CC0206CFE57F841857BF1045FE189593A4F
SHA-512:	295E0EEF7A5FDE8782C936AFE48660343C0AC11AAC04035D4680F3A0375F307004DBE6FE4653A2D2B445D67AC821B53938660132CBC40286456FD2EBFFDE67D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.gxgt.+gt.+gt.+...*mt.+...*.t.+...*st.+5..*At.+5..*vt.+5..*ut.+...*dt.+ gt.+0t.+...*ft.+...+ft.+gt.+ft.+...*ft.+Richgt.+.....PE..L...:T.a.....@.....3.....L..... .....L-..... .....v.....@.....`.....*...z.....@.....@.....@....rsrc..... .....@.....f.... .....@....data.....f.....@....adata.....@..... .....

C:\Users\user\Documents\pAAtCUscyqHcA5VRQHk4us_O.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	49152:LFvq6XhmxAO7uJSeWEtTAi1wkECRSqHlxl:pmxAO7Mai1wkECVh
MD5:	FAB86F0D2562E6CD30D8CBC915A05ECC
SHA1:	087DA5278369D0D409B9BC632E4367497D20DEFC
SHA-256:	DBDBCA9CE3B6396791D703BF0528AA0A9CBF5327BCE848F670F4F72D2F4C555B
SHA-512:	0A5DC51347DA855E8BD2432D83445A8D47931936B4E58BE858C6C76B24A1E307B4F43A44DBDA4BE118455CF007D32CDF09C3267352E209FD6E82DB8068F6345
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L...*2.a.....6.....@..... 8.....i?.....p3.`.....3.,..... ...didata..`3.....`.data.....p3.....@....rsrc...,.....3.....@..@.text.....6.0y.....@..... .....L...gs.6W..6G.K1..xy.w ...X....

C:\Users\user\Documents\pjKel8n3jKGt5QmMP3wRcVWp.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7KLcXaoD:J0+oxBeRmR9etdzRxGezH0q72ma+
MD5:	C8DDCE4DE7D2FD26927E6DB3D554AFD0
SHA1:	4C3F77BB7CD753C5F9DB1B780DF00E14D49BB618
SHA-256:	4A47941324BC9F45254B507AA228D2652064B7277C7FCB0674D1E5FE7DC68467
SHA-512:	FB2A5C27B410449BAA3BF9142A38862337E37FD21712AD21C7CDBF3DDBAB76AE4A6153D756B61DB23D9F931D300333BA6B87319F8955E7EEB401D306BC346C 8
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.45 Port 80</address>.</body></html>.

C:\Users\user\Documents\qLKJuutrhi4_ynFfcv4vuxG2.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7KLcXaoD:J0+oxBeRmR9etdzRxGezH0q72ma+
MD5:	C8DDCE4DE7D2FD26927E6DB3D554AFD0
SHA1:	4C3F77BB7CD753C5F9DB1B780DF00E14D49BB618
SHA-256:	4A47941324BC9F45254B507AA228D2652064B7277C7FCB0674D1E5FE7DC68467
SHA-512:	FB2A5C27B410449BAA3BF9142A38862337E37FD21712AD21C7CDBF3DDBAB76AE4A6153D756B61DB23D9F931D300333BA6B87319F8955E7EEB401D306BC346C 8
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.45 Port 80</address>.</body></html>.

C:\Users\user\Documents\qku3YiVhcZIcmDNEbDutTIoi.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:b/D0I7bieAtJl4gcl4LxzuB5IK+hJEacXVeN19xPkNj:b/xAZclKxYIINFefPGj
MD5:	3ECFD5D9F991294510E111DCF96357FD
SHA1:	7B208DA6822F3B04E27F0B1DCE0E48B11D3E7DA7
SHA-256:	9F7FDE5DC8DD5812E5F58AAB39268D6FFB15FD7A1CCD77686FA970EF55693F85
SHA-512:	36DD26FB198A46E7B453BF13D781BB4F3F970368869BBCBC0F5D8472BAC22B42ABCD41705EB0A0F3085079C8CF37E18513BB695F3EA7210C8D622C630C5039C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32....f.....C'B{b.........+..R...d:.....Q..... ....PE..L.....0.....H..... ...@....@.....@.....@.....`.....p..pG..... ...gfids...P.....`BSS.....`.....@....rsrc...pG...p.....@..@BSS.....y...$.....@..... .....on..D.}[A.y[[C%.x..t.k..i...

C:\Users\user\Documents\smNaHML3VmWpMtzp0xKVqAGa.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+knVkmcXaoD:J0+oxBeRmR9etdzRxGezH0qVkmma+
MD5:	D8091F73C4BF1305D90D964B823793F3
SHA1:	1998FE26E850E014602BD5A281B6D5085D2F8E6D

C:\Users\user\Documents\smNaHML3VmWpMtzp0xKVqAGa.exe	
SHA-256:	0BF453D9D207AD23868BC52853C3724FE604625151DBFDA92EED67647851C462
SHA-512:	6BA323F2B059F290B4FD20533889AD90E08D73B20019439F5F24B5993242C6A547977DB735BF3942566F19A8CD8F02781AE7480B31C2E792161F59509FB771EC
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 45.144.225.57 Port 80</address>.</body></html>.

C:\Users\user\Documents\yZeDvYwRNsEq5bdzAW5HeKXc.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:sDkb/ZeGq8iEj7fdbr5IXfPY583mXSt3YiZUhdZEn1SxIpUFeVxxgfuIr4JJT5p3:DcS7BwL350xIpUgjxV9B
MD5:	2D2494A5406DCB5A23AC757EDD7B7344
SHA1:	D6BA507D368BF332C4AD3B37F0C47084FD3C678F
SHA-256:	750F8DFCFD186862CAFC957400B5B807CBA12F745AC5E26A144F44A1DC212F8C
SHA-512:	C744298B33B5A6386B49E3F164923161C2992325A4A03699456D5BD01B76650B4B5EBE5E09B6F2D281E72463C5D2AA31696D8FAE6910F5591141C5D2BABA1E15
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y.S.....0.....5... ...@....@.. ....@.....p5..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....5.....H.....9.....OG..h...t].....g.....y....(.H..*.s.B...Z...**....(i...*f....(j...r-..p(....(k...*f....ol...(m...ol...on ...*.sBG.....*f....ol...r.$.p(....on...*f....o....r.$.p(....on...*f....o....rE%.p(....(k...*.....o....r.%.p(....rq..p(....r...p(....(....on...*f....o....r*&.p(....(k...*f....o....rl&.p(....(k...*f....o....r.&.p(....(k. ..*f....o....ra'.p(....(k...*.~....:#...r.'.p(.....#...(....o....s.....~....*.~....*.~

C:\Users\user\Documents\z55am8ntfc1tzTQLqXuERA8s.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	49152:i+p0eyG6i0tn1oDIbPcyMROF0V7POqqT4xUXZoMNjkximOk0NaizPA:iY0ex6HqDKyi0dGqqT4ejkxw3s
MD5:	93121163AA243AC42A179A08399AEB07
SHA1:	1E5BEC2A61AFF7C1225103559CE3AC05FE3D8FC7
SHA-256:	7CCFDD6FB206ED5410CE2AA681FDFC0548F4C90DB27A9342B293EA35BBA58B85
SHA-512:	D3E93D59D13881ED3F9B029EDC267E227E33A4ACE31728F36919B9668908F50A4FA9B9244E2B45642D6A844D5C9042BF18F98B4868910FFFF82634EB4F1587FE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....Iu7. .....|.O. ....`M..... ..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....3...P.....@.....1.....@....rsrc.....`M.....0.....@....A4SqVtu.....O.....62.....@....ada ta.....S.....6.....@..... .....

C:\Users\user\Documents\zCgmVlJU85h7EoUzOQ69Wnzh.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:t8f39B+OecSnrJYG4oPSidpXPQvzJetHu7MgUEjumXKHt:worJYGPd1PQ7JUaMjEygK
MD5:	2DBF77866712D9EBD57EC65E7C1598A8
SHA1:	25693E771D3D25112FFA7C38875DECD562AC808D
SHA-256:	2E382DCD1F433490E453D5E7E710D2BB821C2DF09F1E16B675EE060D46DA80D6
SHA-512:	609AA7242A8908AD7B59FD5F303492DDF435320106219D9E35F88B6A9976ADC72CA1E72CD17F714D349E430F8A0D330837C81AD947AC62E4DCD2C83D32A2DB
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L...P.....0.....F..... ... .@.....+.....@.....0.....@...D..... ...data.... .....`.shared.....0.....@....rsrc....D...@...D.....@..@.CRT.....x...L.....@..... .....kg...}R..hI.>..H..... .....

\Device\ConDrv	
Process:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4546
Entropy (8bit):	5.060083473559269
Encrypted:	false
SSDEEP:	96:yjUjnIjjjskn/DUD8CtiApkxehrPDh/cRRh9vZEZfN:yjUjIjjjxn/gttiMRrPDh/cPhVZEZV
MD5:	EF0286D779838C086EF1C19A66BD6057
SHA1:	781E687744FCC55B91463E6FF80CC0ACA8DA6F3A
SHA-256:	EC495690DE8A49FE4F7ED813040AE2130BFFAC40C7ED345DA765F12BCF5B6CE6
SHA-512:	894AAFC36068CDCAB0B079BAC8318730D05B083E7E072BD74B62755628A6792988BF365721653DF26F985B16EF7105AB6E83E4171FC11CA90E5A6C738F786762
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE html>.. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->.. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->.. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->.. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->..<head>..<title>Suspected phishing site | Cloudflare</title>..<meta charset="UTF-8" />..<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />..<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />..<meta name="robots" content="noindex, nofollow" />..<meta name="viewport" content="width=device-width,initial-scale=1" />..<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />.. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->..<style type="text/css">body{margin:0;padding:0}<

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.990283922439568
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:	0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
File size:	2831917
MD5:	971e01647fbdc05bef3df71b008e2ca6
SHA1:	d8122ee820db5d937056c2f1fd0b7bbf89d8b9c1
SHA256:	0ca57f85e88001edd67dff84428375de282f0f92e5bef2ded1c03ad2fa7612e
SHA512:	89d409d331ea527570584e9d0f76f48b0ad84f6e85ae90a0446c436078d503a10dbf78fa67bbe14a07d05b0c00e0ecf81c25e1545ced29d7a72a0ea5aa892780
SSDEEP:	49152:xcB7PkZVi7iKiF8cUvFyPj0TbOTDTfr6pKTfHblwVj+jcEwJ84vLRaBtll9mTIGU:xbri7ixZUvFyPj0gnzesrCvLUBsKIA8l
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B...]...B...^...B...]...B...]...B...J...B...B...B...J...B...d...B...d...B....6..B.....B..]D...B..Rich.B.....

File Icon

Icon Hash:	8484d4f2b8f47434

Static PE Info

General

Entrypoint:	0x41910c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED

General

DLL Characteristics:	NX_COMPAT
Time Stamp:	0x5C6ECB00 [Thu Feb 21 16:00:00 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	32569d67dc210c5cb9a759b08da2bdb3

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19745	0x19800	False	0.583438648897	DOS executable (COM)	6.6301384284	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1b000	0x3a98	0x3c00	False	0.3345703125	data	4.39318766185	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x23f0	0x200	False	0.369140625	data	3.30022863793	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.sxdata	0x22000	0x4	0x200	False	0.02734375	data	0.0203931352361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_LNK_INFO, IMAGE_SCN_MEM_READ
.rsrc	0x23000	0xab0	0xc00	False	0.344401041667	data	3.32928574611	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe PID: 7156 Parent PID: 5280

General

Start time:	19:29:29
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\0CA57F85E88001EDD67DFF84428375DE282F0F92E5BEF.exe"
Imagebase:	0x400000
File size:	2831917 bytes
MD5 hash:	971E01647FBDC05BEF3DF71B008E2CA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: setup_install.exe PID: 5976 Parent PID: 7156

General

Start time:	19:29:34
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\setup_install.exe"
Imagebase:	0x400000
File size:	297472 bytes
MD5 hash:	774F0D5B7DC3D2AD9CC4A0D921C9DA8B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 6004 Parent PID: 5976

General

Start time:	19:29:35
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6548 Parent PID: 5976

General

Start time:	19:29:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c arnatic_1.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4964 Parent PID: 5976

General

Start time:	19:29:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c arnatic_2.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: arnatic_1.exe PID: 5768 Parent PID: 6548

General

Start time:	19:29:36
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_1.exe
Wow64 process (32bit):	true
Commandline:	arnatic_1.exe
Imagebase:	0x400000
File size:	729724 bytes
MD5 hash:	6E43430011784CFF369EA5A5AE4B000F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5868 Parent PID: 5976

General

Start time:	19:29:37
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c arnatic_3.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: arnatic_2.exe PID: 4784 Parent PID: 4964

General

Start time:	19:29:37
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_2.exe
Wow64 process (32bit):	true
Commandline:	arnatic_2.exe
Imagebase:	0x400000
File size:	248832 bytes
MD5 hash:	68BC76A5DF7A7C5368E8AC9484584825
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cmd.exe PID: 6576 Parent PID: 5976

General

Start time:	19:29:37
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c arnatic_4.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: arnatic_3.exe PID: 6564 Parent PID: 5868

General

Start time:	19:29:37
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_3.exe
Wow64 process (32bit):	true
Commandline:	arnatic_3.exe
Imagebase:	0x400000
File size:	625152 bytes
MD5 hash:	208EF3505E28717F9227377DA516C109
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000F.00000003.304993413.0000000002480000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000F.00000000.325466872.00000000023E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000F.00000002.424491159.00000000023E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000F.00000002.423380707.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000F.00000000.316957711.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000F.00000000.322961935.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000F.00000000.321122893.00000000023E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6592 Parent PID: 5976

General

Start time:	19:29:37
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c arnatic_5.exe
Imagebase:	0xd80000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: arnatic_4.exe PID: 6568 Parent PID: 6576

General

Start time:	19:29:38
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_4.exe
Wow64 process (32bit):	false
Commandline:	arnatic_4.exe
Imagebase:	0xd30000
File size:	8192 bytes
MD5 hash:	DBC3E1E93FE6F9E1806448CD19E703F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Analysis Process: cmd.exe PID: 4020 Parent PID: 5976

General

Start time:	19:29:38
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c arnatic_6.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: arnatic_5.exe PID: 4816 Parent PID: 6592

General

Start time:	19:29:38

Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS4FBAB23D\arnatic_5.exe
Wow64 process (32bit):	true
Commandline:	arnatic_5.exe
Imagebase:	0xe20000
File size:	860160 bytes
MD5 hash:	4A1A271C67B98C9CFC4C6EFA7411B1DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Disassembly

Code Analysis