ID: 626897
Sample Name:
SecuriteInfo.com.Variant.Jaik.73085.20962.11149
Cookbook: default.jbs
Time: 21:36:22
Date: 15/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

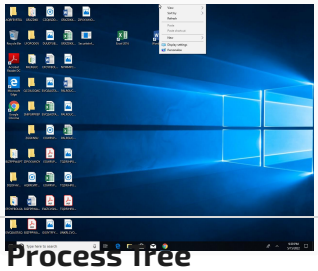
Windows Analysis Report

SecuriteInfo.com.Variant.Jaik.73085.20962.11149

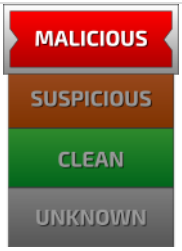
Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.Jaik.73085.20962.11149 (renamed file extension from 11149 to exe)
Analysis ID:	626897
MD5:	35ed3fe203fabde.
SHA1:	6a5e219fd96905..
SHA256:	8d4020bea89243.
Tags:	exe
Infos:	



Detection



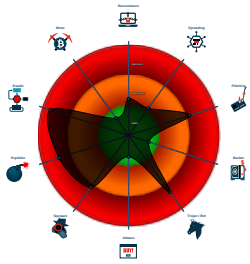
AveMaria, UACMe

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Sigma detected: Drops script at sta…
- Multi AV Scanner detection for drop…
- Detected unpacking (creates a PE f…
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Writes to foreign memory regions
- Increases the number of concurrent…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Variant.Jaik.73085.20962.exe (PID: 5708 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe" MD5: 35ED3FE203FABDE1B0D353815F9A273B)
  - powershell.exe (PID: 5900 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - windowupdate.exe (PID: 5732 cmdline: C:\ProgramData\windowupdate.exe MD5: 35ED3FE203FABDE1B0D353815F9A273B)
    - powershell.exe (PID: 316 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 4240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 1636 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 3116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 6080 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat" " MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 2460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WMIC.exe (PID: 5596 cmdline: wmic process call create '"C:\ProgramData:ApplicationData"' MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
- WmiPrvSE.exe (PID: 1824 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "104.128.191.44",
  "port": 8080
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.310084355.0000000001080000.00000004.00000020.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x4fd0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x4fd0:$c1: Elevation:Administrator!new:
00000003.00000003.310084355.0000000001080000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
00000003.00000003.310084355.0000000001080000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000003.310084355.0000000001080000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000000.00000003.271131507.0000000000E95000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 45 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.windowupdate.exe.1084250.2.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
3.3.windowupdate.exe.1084250.2.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:
3.3.windowupdate.exe.1084250.2.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
3.3.windowupdate.exe.10be378.0.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
3.3.windowupdate.exe.10be378.0.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:
Click to see the 97 entries				

Sigma Signatures

Data Obfuscation

Sigma detected: Drops script at startup location

Snort Signatures

ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound) - Source IP: 104.128.191.44 - Destination IP: 192.168.2.3 −

Timestamp:	104.128.191.44192.168.2.38080496942841903 05/15/22-21:37:58.748904
SID:	2841903
Source Port:	8080
Destination Port:	49694
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin - Source IP: 192.168.2.3 - Destination IP: 104.128.191.44 −

Timestamp:	192.168.2.3104.128.191.444969480802834979 05/15/22-21:37:58.879218
SID:	2834979
Source Port:	49694
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Exploits

Yara detected UACMe UAC Bypass tool

Compliance

Detected unpacking (creates a PE file in dynamic memory)

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

E-Banking Fraud

Yara detected AveMaria stealer

System Summary

Malicious sample detected (through community Yara rule)

Contains functionality to create processes via WMI

Data Obfuscation

Detected unpacking (creates a PE file in dynamic memory)

Persistence and Installation Behavior

Creates processes via WMI

Boot Survival

Drops script or batch files to the startup folder

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

Creates files in alternative data streams (ADS)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information

Yara detected AveMaria stealer

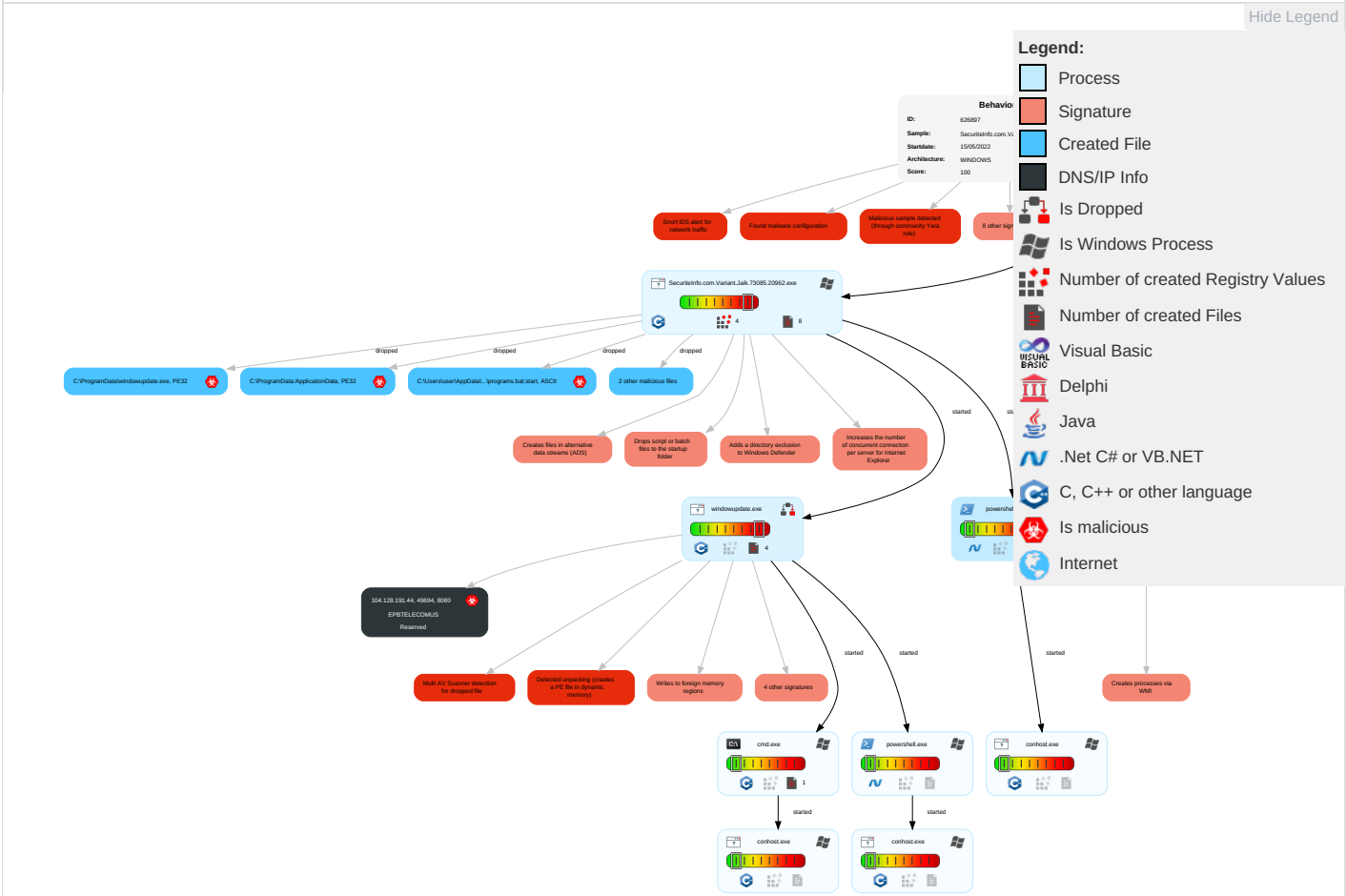
Remote Access Functionality

Yara detected AveMaria 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 1 Windows Management Instrumentation	2 Registry Run Keys / Startup Folder	3 1 2 Process Injection	1 1 Disable or Modify Tools	1 1 1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Endpoint Denial of Service
Default Accounts	1 1 Scripting	Boot or Logon Initialization Scripts	2 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 1 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Scripting	Security Account Manager	1 5 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Software Packing	LSA Secrets	1 2 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 Masquerading	Cached Domain Credentials	2 Process Discovery	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	2 1 Virtualization/Sandbox Evasion	DCSync	2 1 Virtualization/Sandbox Evasion	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	3 1 2 Process Injection	Proc Filesystem	1 Application Window 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)	1 Hidden Users	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 NTFS File Attributes	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

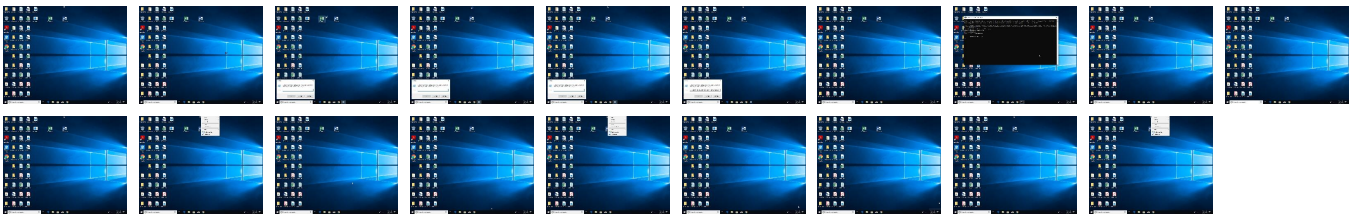
Behavior Graph



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
SecuriteInfo.com.Variant.Jaik.73085.20962.exe	17%	ReversingLabs	Win32.Trojan.Jaik	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData:ApplicationData	17%	ReversingLabs	Win32.Trojan.Jaik	
C:\ProgramData\windowupdate.exe	17%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.3.windowupdate.exe.10928d8.10.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
3.3.windowupdate.exe.10928d8.12.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
3.2.windowupdate.exe.38d0000.3.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
0.2.SecuriteInfo.com.Variant.Jaik.73085.20962.exe.3460000.3.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.3.windowupdate.exe.10928d8.4.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
3.2.windowupdate.exe.2ed053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Variant.Jaik.73085.20962.exe.2a6053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
3.3.windowupdate.exe.10928d8.5.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
104.128.191.44	0%	Avira URL Cloud	safe	
http://crl.m	0%	URL Reputation	safe	
http://https://ion=v4.5n	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

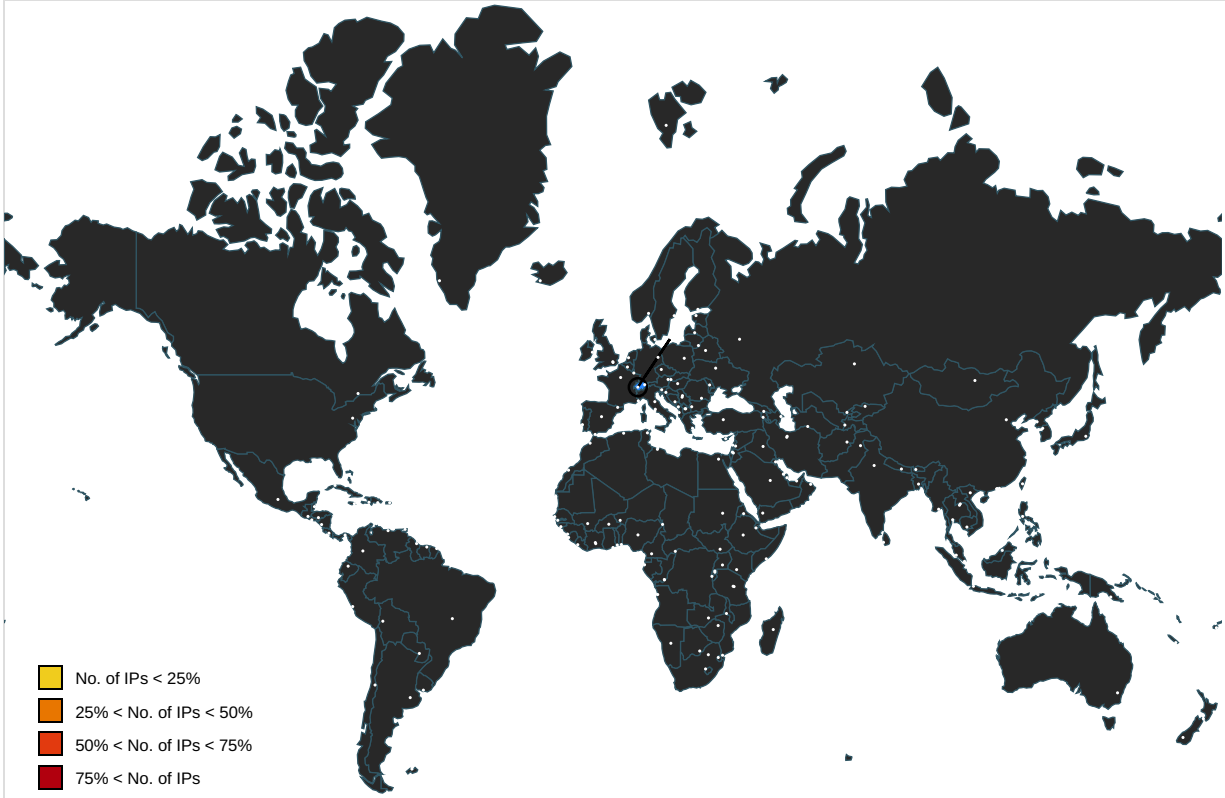
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
104.128.191.44	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.m	powershell.exe, 0000000D.00000003.411093654.000000000917F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ion=v4.5n	powershell.exe, 00000001.00000003.382885100.0000000007B91000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000003.385315234.0000000007BAF000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000003.383555084.0000000007BAE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://github.com/syohex/java-simple-mine-sweeperC:	SecuriteInfo.com.Variant.Jaik.73085.20962.exe, 00000000.00000002.298458664.000000003474000.00000002.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Jaik.73085.20962.exe, 00000000.00000002.297237993.0000000002A60000.00000040.00001000.00020000.00000000.sdmp, windowupdate.exe, 00000003.00000002.525655922.00000000038E4000.00000002.00001000.00020000.00000000.sdmp, windowupdate.exe, 00000003.00000002.525427546.000000002ED0000.00000040.00001000.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000001.00000002.389408114.00000000045EE000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.412976315.0000000004783000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000001.00000002.388775306.00000000044B1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.412820303.0000000004641000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000001.00000002.389408114.00000000045EE000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.412976315.0000000004783000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.128.191.44	unknown	Reserved	?	26827	EPBTELECOMUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626897
Start date and time: 15/05/202221:36:22	2022-05-15 21:36:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Jaik.73085.20962.11149 (renamed file extension from 11149 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
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.phis.troj.spyw.expl.evad.winEXE@17/14@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 84.4% (good quality ratio 83%) • Quality average: 83.8% • Quality standard deviation: 20.4%
HCA Information:	• Successful, ratio: 79% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.

Simulations

Behavior and APIs

Time	Type	Description
21:37:41	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat
21:37:52	API Interceptor	1x Sleep call for process: WMIC.exe modified
21:37:58	API Interceptor	806x Sleep call for process: cmd.exe modified
21:38:01	API Interceptor	47x Sleep call for process: powershell.exe modified

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:\ProgramData:ApplicationData

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	2054656
Entropy (8bit):	4.278811521243932

Encrypted:	false
SSDEEP:	12288:ed05fRBi1vvXHdJUNoyiiguuJ2glmnGeNCrRcQc/PJcEj2uGn9bunQ7JiD4pa7+o:q1vfHUorlm9NCFcR/PJc4gbunQ
MD5:	35ED3FE203FABDE1B0D353815F9A273B
SHA1:	6A5E219FD96905B154295697AC6F72A13725F6A1
SHA-256:	8D4020BEA8924365724FF2C7EAFFA0541F0AC4712C6B0A4723C5F68858FA306C
SHA-512:	9657C11D07068F9E054BC701A0789E3918E4554F845B6CF6371299CE477FB17CEF6F4AB97469BECB5892BB66091435E1BFB187299A8D6722564813EC767B4CBB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 17%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D.j.*.j.*.j.*...).g.*.../...*.....z.*...).~.*.../.V.*.....~.*...+.e.*.j.+..*...# .n.*....k.*.j...k.*...(.k.*.Richj.*.....PE..L....?|b.....H...B.....`....@.....@.....G.....@..@.....`..`.....T..... .....@.....`.....text....H.....H..... ..`.rdata.....`.....L.....@..@.data.....`.....B.....@....rsrc...@....@.....@..@.reloc... `..`...b.....@..B..... .....

C:\ProgramData\windowupdate.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2054656
Entropy (8bit):	4.278811521243932
Encrypted:	false
SSDEEP:	12288:ed05fRBi1vvXHdJUNoyiiguuJ2glmnGeNCrRcQc/PJcEj2uGn9bunQ7JiD4pa7+o:q1vfHUorlm9NCFcR/PJc4gbunQ
MD5:	35ED3FE203FABDE1B0D353815F9A273B
SHA1:	6A5E219FD96905B154295697AC6F72A13725F6A1
SHA-256:	8D4020BEA8924365724FF2C7EAFFA0541F0AC4712C6B0A4723C5F68858FA306C
SHA-512:	9657C11D07068F9E054BC701A0789E3918E4554F845B6CF6371299CE477FB17CEF6F4AB97469BECB5892BB66091435E1BFB187299A8D6722564813EC767B4CBB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 17%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D.j.*.j.*.j.*...).g.*.../...*.....z.*...).~.*.../.V.*.....~.*...+.e.*.j.+..*...# .n.*....k.*.j...k.*...(.k.*.Richj.*.....PE..L....?|b.....H...B.....`....@.....@.....G.....@..@.....`..`.....T..... .....@.....`.....text....H.....H..... ..`.rdata.....`.....L.....@..@.data.....`.....B.....@....rsrc...@....@.....@..@.reloc... `..`...b.....@..B..... .....

C:\ProgramData\windowupdate.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:wZvOdB8Ypib4JNXp59HopbjvwRjdvRlAYotiQ0HzAF8:UvOdB8YNNZjHopbjoRjdvRlAYotinHzr
MD5:	C5A56B913DEEDCF5AE01A2D4F8AA69CE
SHA1:	C91D19BFD666FDD02B0739893833D4E1C0316511
SHA-256:	1C5C865E5A98F33E277A81FCDADFBAB1367176BA14F8590022F7E5880161C00D

SHA-512:	1058802FCD54817359F84977DD26AD4399C572910E67114F70B024EBADDF4E35E6AFF6461F90356205228B4B860E69392ABC27D38E284176C699916039CFA5ED
Malicious:	false
Preview:	PSMODULECACHE.....#y;...Q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1.....Start-BitsTransfer.....Set-BitsTransfer .....Get-BitsTransfer.....Resume-BitsTransfer.....Add-BitsFile.....Suspend-BitsTransfer.....Complete-BitsTransfer.....Remove-BitsTransfer.....-.^(...[...C:\Win dows\system32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1....#...Set-AppBackgroundTaskResourcePolicy.....Unregister-App BackgroundTask.....Get-AppBackgroundTask.....tid.....pfn.....iru....%...Enable-AppBackgroundTaskDiagnosticLog.....Start-AppBackgroundTask....&...Disable-Ap pBackgroundTaskDiagnosticLog.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1..... ..Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Pac kage.....Unins

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21540
Entropy (8bit):	5.601157753176713
Encrypted:	false
SSDEEP:	384:wtL6/0UWqENJ82XRYSBKnWZispE93C1u16zq5mHKHyQ3DrjaIvUI++j/:SHH8v4KWlwC3qUZGX2ly
MD5:	29B2B467A2C4A48C8645FF0AA566BEB2
SHA1:	C043EEA8A352A9A4A80B27AFF10B94017E98258C
SHA-256:	192DEC31FD6C2C952502D10D265BA639BA30A3F18172A734D18E807BE65A318A
SHA-512:	A83E902CBD5D128E75F4E45085F9DA6B80D6442529628CA2F59DAAA69C33A63AA661D9B9D22A3215E2FC9B6B3B23B34A83402DB71FFCF93964BCC4572B6DDE 47
Malicious:	false
Preview:	@...e.....@.....H.....<@.^.L."My...:=.... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)Q.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,j.....(.Microsoft.PowerShell.Commands.ManagementT.....7.,.fiD..... .....*.Microsoft.Management.Inf

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0xfmcqke.tvf.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pyoxucyx.042.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qeiqozgs.3mq.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tacmmont.cza.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	140
Entropy (8bit):	4.86129651314522
Encrypted:	false
SSDEEP:	3:QwZ2vOUrKaM6eNGRjDWXp5cViEaKC5SufyM1K/RFofD6tRQLRWLyLRHgn:QElPhxuWXp+NaZ5SuH1MUmt2FWLyS
MD5:	C2E52EDB9BA6919C7D9F3CF0B88221E2
SHA1:	9972112AF86B48E937E589E262D21BAD251A6010
SHA-256:	FAE189421B6E7CC977F1D2A69D712C97B22E810B0AE3F2F4E258E1112694C560
SHA-512:	FDDEDA3E5D597D086B9C4412621078B3D14B6624DF2B003CA3238E3BD03DE35AAF3E16F04339AC54B04A723F98E76F17D74263F7D1CCBCA92B6FD2C325014BB
Malicious:	**true**
Preview:	for /F "usebackq tokens=*" %%A in ("C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat:start") do %%A

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat:start	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.2659637614761765
Encrypted:	false
SSDEEP:	3:eGAjGJwbZkREfcjMGERMQhM:ZuGJwi8cwGj
MD5:	579E29CEC6BDE04C5C074D8311D6B884
SHA1:	2FDFD4C6B8EB43A4C6F4C0D3998E4A5364221DFF
SHA-256:	65138897F467ADF9FE20594326D724D2CD5B437D9AACF5F83721AF340F70CE3C

SHA-512:	4011A9FD58C1DC8AA3ED79589D7232BBD06EB3FB32513D3C5B59B740ED89FDC9CCC9F3291812AFFF2CD679820BCD940AE3A49E41EBCBE20413821ACAD7C591D
Malicious:	**true**
Preview:	wmic process call create "'C:\ProgramData:ApplicationData"'

C:\Users\user\Documents\20220515\PowerShell_transcript.910646.QaUfbtTD.20220515213758.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5045
Entropy (8bit):	5.388024296986314
Encrypted:	false
SSDEEP:	96:BZmhQN5QqDo1ZBZFhQN5QqDo1ZqM6UjZVhQN5QqDo1ZwFEEqZN:9FTM
MD5:	3E07E8924F7C65A903A2367B78CDBF93
SHA1:	3DC700FAE2312E5FE2DA6F97838BF44E2EB7331F
SHA-256:	459AC2BFD4CEA72230ACD72E11C941AA174D7820420FEE8C132DF10E4316392F
SHA-512:	2FF33B7E0CECD2FBD94B5F0EB6882CD8A323E253F6DA74F83034889DBAAB07BA22E7B8FAD73804807619DB6C42A34CBC829A4759697973364DA3843952B2451
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220515213818..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -ExclusionPath C:\..Process ID: 316..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220515213818..**********..PS>Add-MpPreference -ExclusionPath C:\..**********..Windows PowerShell transcript start..Start time: 20220515214218..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -Exclusi

C:\Users\user\Documents\20220515\PowerShell_transcript.910646.TABzkN2n.20220515213740.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5048
Entropy (8bit):	5.388063371930918
Encrypted:	false
SSDEEP:	96:BZePhQN5sqDo1ZIwZ6hQN5sqDo1ZQM6UjZnhQN5sqDo1ZTFEEjZl:iSdKPq
MD5:	A7C69A3C25CAFBE9F023AFF815477553
SHA1:	27F02E22876CA925486635A175E81C7B7593A9F4
SHA-256:	0079DBBC9539A71EB85FE5F33FE64A8F6E0EB2B07ED1C73E060CF0FC9FCFE19B
SHA-512:	37523698E4897E3B3F70DD8541E21953C953AAA8DFED9BBF4C1F47C7188F42810DBB26880B3740A5281631F06B346B7A59553DF83533A9A8D781C906362DC3F0
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220515213757..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -ExclusionPath C:\..Process ID: 5900..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220515213757..**********..PS>Add-MpPreference -ExclusionPath C:\..**********..Windows PowerShell transcript start..Start time: 20220515214020..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -Exclus

\Device\ConDrv

Process:	C:\Windows\System32\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	140
Entropy (8bit):	5.001523394375711
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys36JQAimXv:Yw7gJGWMXJXKSOdYiygKkXe/qeAiY
MD5:	DA5950D62F7968DA1F66E3811A9061F9
SHA1:	69B83F624AA9EC9EA09BE0E165499B436101F9EA
SHA-256:	C09AF5F39B8BF613C007465A63F70E84766710CEE7FEB62780433C9D8C248AD7
SHA-512:	6291C46BC66AEC7AEB973EE076146AF54C800A63F3F6F9C0EF01DA6535539E2F44FBF0BACBEAF66C4D34C4BE122AD728F62681E408FA710127120806D952DC9E
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ReturnValue = 9;..};....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.278811521243932
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:	SecuriteInfo.com.Variant.Jaik.73085.20962.exe
File size:	2054656
MD5:	35ed3fe203fabde1b0d353815f9a273b
SHA1:	6a5e219fd96905b154295697ac6f72a13725f6a1
SHA256:	8d4020bea8924365724ff2c7eaffa0541f0ac4712c6b0a4723c5f68858fa306c
SHA512:	9657c11d07068f9e054bc701a0789e3918e4554f845b6cf6371299ce477fb17cef6f4ab97469becb5892bb66091435e1bfb187299a8d6722564813ec767b4cbb
SSDEEP:	12288:ed05fRBi1vvXHdJUNoyiiguuJ2glmnGeNCrRcQc/PJcEj2uGn9bunQ7JiD4pa7+o:q1vfHUorlm9NCFcR/PJc4gbunQ
TLSH:	47951910B3A15124F5F767FA66B54694887E3C811F2CE2CF4A850ADECA292F47C347A7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D.j.*.j.*.j.*...).g.*.../...*.....z.*...).~.*.../.V.*.....~.*...+.e.*.j.+...*...#.n.*.....k.*.j...k.*...(.k.*.Richj.*.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4187d0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627C3FE2 [Wed May 11 22:59:46 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	f40b392a15f243aae9f6b24f04047e6e

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
call 00007F63D0CF1EEDh
pop ebp
ret
int3
int3
int3
int3
int3

Instruction
int3
push ebp
mov ebp, esp
push ecx
mov dword ptr [ebp-04h], ecx
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+08h]
mov ecx, dword ptr [eax]
mov dword ptr [ebp-04h], ecx
mov eax, dword ptr [ebp-04h]
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007F63D0CF2189h
add esp, 04h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007F63D0CF2249h
add esp, 04h
test eax, eax
je 00007F63D0CF21B3h
int3
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007F63D0CF2229h
add esp, 04h
test eax, eax
je 00007F63D0CF21B9h
mov ecx, 00000041h
int 29h
pop ebp
ret
int3
int3
int3
int3
push ebp
mov ebp, esp
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007F63D0CF21F9h
add esp, 04h
test eax, eax

Instruction
je 00007F63D0CF21BEh
mov ecx, dword ptr [ebp+08h]
push ecx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc4780	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1f4000	0x1040	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1f6000	0x60c4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc1398	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc1480	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xc12d8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x96000	0x2b0	.rdata
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	0x94800	0x94800	False	0.348802149095	data	6.1898202899	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x96000	0x2f5f0	0x2f600	False	0.203645489776	data	4.42534631821	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc6000	0x12d7e0	0x12a400	False	0.134401358183	data	2.31170755301	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1f4000	0x1040	0x1200	False	0.351345486111	data	3.69129058144	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1f6000	0x60c4	0x6200	False	0.742665816327	data	6.70176669915	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
TYPELIB	0x1f4190	0x834	data	English	United States
RT_DIALOG	0x1f4ce0	0x1ae	data	English	United States
RT_STRING	0x1f4e90	0x2e	data	English	United States
RT_VERSION	0x1f49c8	0x314	data	English	United States
RT_MANIFEST	0x1f4ec0	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetModuleHandleA, HeapSize, GetCommandLineA, MultiByteToWideChar, Sleep, GetLastError, SetEvent, LockResource, HeapReAlloc, RaiseException, FindResourceExW, IsDBCSLeadByte, LoadResource, FindResourceW, HeapAlloc, DecodePointer, HeapDestroy, GetProcAddress, DeleteCriticalSection, GetProcessHeap, GetModuleHandleW, WideCharToMultiByte, lstrcmpiA, TlsFree, CreateFileW, ReadConsoleW, GetCurrentThreadId, FlushFileBuffers, GetConsoleMode, GetConsoleCP, SetFilePointerEx, GetFileSizeEx, GetStringTypeW, SetStdHandle, SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, FindFirstFileExW, FindClose, HeapQueryInformation, SetConsoleCtrlHandler, WriteConsoleW, GetFileType, GetCurrentThread, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, InitializeCriticalSectionEx, GetModuleFileNameA, LeaveCriticalSection, VirtualAlloc, EnterCriticalSection, SetLastError, HeapFree, VirtualProtect, SizeofResource, ReadFile, GetLocaleInfoW, LCMapStringW, CompareStringW, GetTimeFormatW, GetDateFormatW, WriteFile, GetStdHandle, ExitProcess, HeapValidate, GetModuleHandleExW, GetModuleFileNameW, VirtualQuery, GetSystemInfo, TlsSetValue, TlsGetValue, TlsAlloc, InterlockedFlushSList, RtlUnwind, GetSystemTimeAsFileTime, GetCurrentProcessId, QueryPerformanceCounter, GetStartupInfoW, TerminateProcess, SetUnhandledExceptionFilter, LoadLibraryExW, EncodePointer, InitializeSListHead, InterlockedPopEntrySList, InterlockedPushEntrySList, GetCurrentProcess, FlushInstructionCache, IsProcessorFeaturePresent, VirtualFree, LoadLibraryExA, IsDebuggerPresent, OutputDebugStringW, CloseHandle, InitializeCriticalSectionAndSpinCount, ResetEvent, WaitForSingleObjectEx, CreateEventW, UnhandledExceptionFilter, FreeLibrary
USER32.dll	CharUpperA, CreateDialogParamA, CharNextW, UnregisterClassA, SetWindowLongA, PostThreadMessageA, IsWindow, ShowWindow, MessageBoxA, GetClientRect, DestroyWindow, GetWindow, GetWindowRect, GetDC, SetWindowPos, MonitorFromWindow, MapWindowPoints, GetWindowLongA, DispatchMessageA, GetMonitorInfoA, GetParent, ReleaseDC, IsWindowVisible, SendMessageA, GetDlgItem, EnableWindow, CharNextA, GetMessageA
GDI32.dll	GetTextExtentPoint32A
ADVAPI32.dll	RegCloseKey, RegDeleteKeyA, RegCreateKeyExA, RegEnumKeyExA, RegQueryInfoKeyA, RegOpenKeyExA, RegSetValueExA
SHELL32.dll	SHGetFileInfoA
ole32.dll	StringFromGUID2, CoAddRefServerProcess, CoReleaseServerProcess, StringFromCLSID, CoInitialize, CoRevokeClassObject, CoUninitialize, CoCreateInstance, CoTaskMemFree, CoRegisterClassObject
OLEAUT32.dll	SysAllocStringLen, UnRegisterTypeLib, LoadRegTypeLib, LoadTypeLib, VariantInit, RegisterTypeLib, SysAllocString, SysStringLen, VarUI4FromStr, SysFreeString, SetErrorInfo, CreateErrorInfo

Version Infos

Description	Data
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	ATLDUCK
FileVersion	1, 0, 0, 1
CompanyName	
ProductName	atlduck Module
OLESelfRegister	
ProductVersion	1, 0, 0, 1
FileDescription	atlduck Module
OriginalFilename	ATLDUCK.DLL
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Snort IDS Alerts

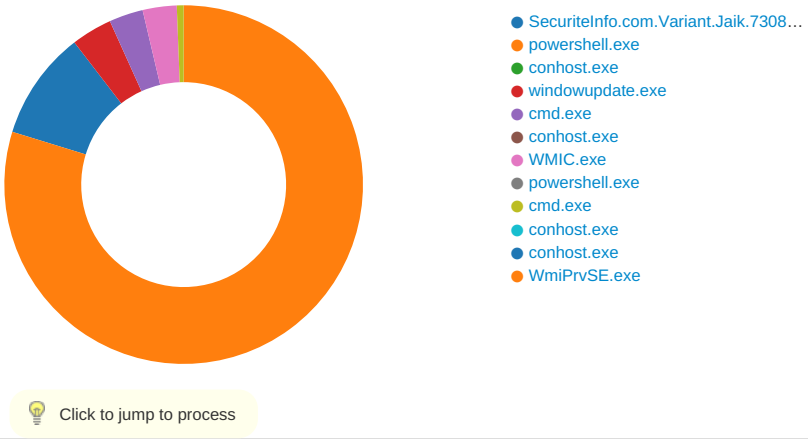
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
104.128.191.44192.168.2.38080496942841903 05/15/22-21:37:58.748904	TCP	2841903	ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)	8080	49694	104.128.191.44	192.168.2.3
192.168.2.3104.128.191.444969480802834979 05/15/22-21:37:58.879218	TCP	2834979	ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin	49694	8080	192.168.2.3	104.128.191.44

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 15, 2022 21:37:58.681555033 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:37:58.714667082 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:37:58.715264082 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:37:58.748903990 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:37:58.874927044 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:37:58.879218102 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:37:58.966294050 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:37:58.966352940 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:37:59.051170111 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:38:18.746695042 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:38:18.750108957 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:38:18.846959114 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:38:38.766438961 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:38:38.767307997 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:38:38.844547033 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:38:58.778517962 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:38:58.779375076 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:38:58.856599092 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:39:18.791378021 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:39:18.796629906 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:39:18.874511957 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:39:38.810094118 CEST	8080	49694	104.128.191.44	192.168.2.3
May 15, 2022 21:39:38.810285091 CEST	49694	8080	192.168.2.3	104.128.191.44
May 15, 2022 21:39:38.894669056 CEST	8080	49694	104.128.191.44	192.168.2.3

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Variant.Jaik.73085.20962.exe PID: 5708, Parent PID: 3068

General

Target ID:	0
Start time:	21:37:28
Start date:	15/05/2022

Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe"
Imagebase:	0x940000
File size:	2054656 bytes
MD5 hash:	35ED3FE203FABDE1B0D353815F9A273B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.271131507.0000000000E95000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.271131507.0000000000E95000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.271032927.0000000000E95000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.271032927.0000000000E95000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.271032927.0000000000E95000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.271032927.0000000000E95000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.271207797.0000000000E90000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.271207797.0000000000E90000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.298671123.00000000035AF000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.298671123.00000000035AF000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.271113826.0000000000EA5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.271113826.0000000000EA5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.298458664.0000000003474000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.298458664.0000000003474000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.297237993.0000000002A60000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.297237993.0000000002A60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.297237993.0000000002A60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.297237993.0000000002A60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.271046859.0000000000EA5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.271046859.0000000000EA5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	347360F	CreateDirectoryW
C:\ProgramData\windowupdate.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	34711DD	CopyFileW
C:\ProgramData\windowupdate.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	34711DD	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3471D55	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat:start	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3471D55	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData:ApplicationData	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	3471388	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\windowupdate.exe	0	262144	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 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 2e fd 44 fd 6a fd 2a fd 6a fd 2a fd 6a fd 2a fd 0f fd 29 fd 67 fd 2a fd 0f fd 2f fd fd fd 2a fd 08 fd 2e fd 7a fd 2a fd 08 fd 29 fd 7e fd 2a fd 08 fd 2f fd 56 fd 2a fd 0f fd 2e fd 7e fd 2a fd 0f fd 2b fd 65 fd 2a fd 6a fd 2b fd e2 2a fd fd fd 23 fd 6e fd 2a fd fd fd 53 6b fd 2a fd 6a fd fd fd 6b fd 2a fd fd fd 28 fd 6b fd 2a fd 52 69 63 68 6a fd 2a fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$.Dj*j*j*)g*/*.z*)~*/*.~*+e*j+*#n*k*jk*(k*Richj*	success or wait	8	34711DD	CopyFileW
C:\ProgramData\windowupdate.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	34711DD	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	0	140	66 6f 72 20 2f 46 20 22 75 73 65 62 61 63 6b 71 20 74 6f 6b 65 6e 73 3d 2a 22 20 25 25 41 20 69 6e 20 28 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 53 74 61 72 74 20 4d 65 6e 75 5c 50 72 6f 67 72 61 6d 73 5c 53 74 61 72 74 75 70 5c 70 72 6f 67 72 61 6d 73 2e 62 61 74 3a 73 74 61 72 74 22 29 20 64 6f 20 25 25 41	for /F "usebackq tokens=*" %%A in ("C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat:start") do %%A	success or wait	1	3471D6C	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat:start	0	59	77 6d 69 63 20 70 72 6f 63 65 73 73 20 63 61 6c 6c 20 63 72 65 61 74 65 20 27 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 3a 41 70 70 6c 69 63 61 74 69 6f 6e 44 61 74 61 22 27	wmic process call create '"C:\ProgramData:ApplicationData"'	success or wait	1	3471D6C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData:ApplicationData	0	262144	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 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 2e fd 44 fd 6a fd 2a fd 6a fd 2a fd 6a fd 2a fd 0f fd 29 fd 67 fd 2a fd 0f fd 2f fd fd fd 2a fd 08 fd 2e fd 7a fd 2a fd 08 fd 29 fd 7e fd 2a fd 08 fd 2f fd 56 fd 2a fd 0f fd 2e fd 7e fd 2a fd 0f fd 2b fd 65 fd 2a fd 6a fd 2b fd e2 2a fd fd fd 23 fd 6e fd 2a fd fd fd 53 6b fd 2a fd 6a fd fd fd 6b fd 2a fd fd fd 28 fd 6b fd 2a fd 52 69 63 68 6a fd 2a fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$.Dj*j*j*)g*/*. z*)~*/*.~*+e*j+*#n*k*jk* (k*Richj*	success or wait	8	3471388	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.73085.20962.exe	unknown	2054656	success or wait	1	3471E78	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\A2U8VJ2CY0	success or wait	1	3470F94	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPer1_0Server	dword	10	success or wait	1	3473572	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPerServer	dword	10	success or wait	1	3473587	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\A2U8VJ2CY0	inst	binary	29 09 31 D9 56 2C 26 1E A6 47 DF F5 F1 40 8E C0 29 14 75 21 3B FC 5E C7 42 27 7A AC 4C 58 CF 89 06 7D 73 A7 70 FB 70 E2 53 B1 E7 CD 6E 08 2A CA 76 0E EF F4 62 1D EA 54 F9 78 CF 7F E3 D4 D0 29	success or wait	1	347105E	RegSetValueExW

Analysis Process: powershell.exe PID: **5900**, Parent PID: **5708**

General

Target ID:	1
Start time:	21:37:36
Start date:	15/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x9b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

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	6DA6CF06	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	6DA6CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_tacmmont.cza.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C151E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pyoxucyx.042.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C151E60	CreateFileW
C:\Users\user\Documents\20220515	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C15BEFF	CreateDirectoryW
C:\Users\user\Documents\20220515\PowerShell_transcript.910646.TABzkN2n.20220515213740.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C151E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_tacmmont.cza.ps1	success or wait	1	6C156A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pyoxucyx.042.psm1	success or wait	1	6C156A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_tacmmont.cza.ps1	0	1	31	1	success or wait	1	6C151B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pyoxucyx.042.psm1	0	1	31	1	success or wait	1	6C151B4F	WriteFile
C:\Users\user\Documents\20220515\PowerShell_transcript.910646.TABzkN2n.20220515213740.txt	0	3	ff		success or wait	1	6C151B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220515\PowerShell_transcript.910646.TABzkN2n.20220515213740.txt	3	588	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 35 32 31 33 37 35 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 39 31 30 36 34 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220515213757Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 910646 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	6C151B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 fd 23 79 3b 9f fd 08 51 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 42 69 74 73 54 72 61 6e 73 66 65 72 5c 42 69 74 73 54 72 61 6e 73 66 65 72 2e 70 73 64 31 08 00 00 00 12 00 00 00 53 74 61 72 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 10 00 00 00 53 65 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 10 00 00 00 47 65 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 13 00 00 00 52 65 73 75 6d 65 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 0c 00 00 00 41 64 64 2d 42 69 74 73 46 69 6c 65 08 00 00 00 14 00 00 00 53 75 73 70 65 6e 64 2d 42 69 74 73 54 72 61	PSMODULECACHE#y;QC:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1Start-BitsTransferSet-BitsTransferGet-BitsTransferResume-BitsTransferAdd-BitsFileSuspend-BitsTra	success or wait	1	6C151B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 42 69 74 4c 6f 63 6b 65 72 5c 42 69 74 4c 6f 63 6b 65 72 2e 70 73 6d 31 28 00 00 00 20 00 00 00 41 64 64 2d 45 78 74 65 72 6e 61 6c 4b 65 79 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 19 00 00 00 43 6c 65 61 72 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74 6f 55 6e 6c 6f 63 6b 02 00 00 00 1b 00 00 00 44 69 73 61 62 6c 65 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74 6f 55 6e 6c 6f 63 6b 02 00 00 00 1b 00 00 00 47 65 74 2d 42 69 74 4c 6f 63 6b 65 72 56 6f 6c 75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 1b 00 00 00 53 65 74 2d 42 69 74 4c 6f 63 6b 65 72 56 6f 6c 75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 45 6e 61 62 6c 65 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74	wsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1(Add-ExternalKeyProtectorInternalClear-BitLockerAutoUnlockDisable-BitLockerAutoUnlockGet-BitLockerVolumeInternalSet-BitLockerVolumeInternalEnable-BitLockerAut	success or wait	1	6C151B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	4096	72 64 08 00 00 00 0d 00 00 00 53 74 61 72 74 2d 50 72 6f 63 65 73 73 08 00 00 00 0b 00 00 00 49 6e 76 6f 6b 65 2d 49 74 65 6d 08 00 00 00 0d 00 00 00 53 74 6f 70 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 09 00 00 00 4a 6f 69 6e 2d 50 61 74 68 08 00 00 00 0c 00 00 00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 1a 00 00 00 54 65 73 74 2d 43 6f 6d 70 75 74 65 72 53 65 63 75 72 65 43 68 61 6e 6e 65 6c 08 00 00 00 0e 00 00 00 4c 69 6d 69 74 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 10 00 00 00 49 6e 76 6f 6b 65 2d 57 6d 69 4d 65 74 68 6f 64 08 00 00 00 10 00 00 00 47 65 74 2d 49 74 65 6d 50 72 6f 70 65 72 74 79 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0b 00 00 00 4e 65	rdStart-ProcessInvoke-ItemStop-ComputerGet-HotFixJoin-PathStop-ProcessTest-ComputerSecureChannelLimit-EventLogInvoke-WmiMethodGet-ItemPropertyRemove-ComputerNe	success or wait	1	6C151B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	12288	2446	3b 9f fd 08 71 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 00 08 00 00 00 47 65 74 2d 44 61 74 65 08 00 00 00 0e 00 00 00 43 6c 65 61 72 2d 56 61 72 69 61 62 6c 65 08 00 00 00 13 00 00 00 47 65 74 2d 45 76 65 6e 74 53 75 62 73 63 72 69 62 65 72 08 00 00 00 0a 00 00 00 49 6d 70 6f 72 74 2d 43 73 76 08 00 00 00 0c 00 00 00 47 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0c 00 00 00 4e 65 77 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f	;qC:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mGet-DateClear-VariableGet-EventSubscriberImport-CsvGet-VariableNew-VariableCo	success or wait	1	6C151B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 13 00 00 18 00 00 00 fd 0b fd 03 fd 07 fd 07 fd 07 00 00 00 00 fd 00 17 00 fd 0b 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	6DD376FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 3d 00 00 00 0e 00 20 00	H<@^L"My:=	success or wait	17	6DD376FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DD376FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DD376FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DD376FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 fd 00 40 00 fd 67 40 01 fd 01 40 00 fd 00 40 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 00 01 fd 44 00 01 fd 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00	@g@@@T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;MDD@M<M$M8M?MBMDmEEMqqS%	success or wait	11	6DD376FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA4CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA4CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA45705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DA51F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6DA5203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9A03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C151B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA45705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	56	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C151B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C151B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C151B4F	ReadFile

Analysis Process: conhost.exe PID: **5912**, Parent PID: **5900**

General

Target ID:	2
Start time:	21:37:37
Start date:	15/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: windowupdate.exe PID: **5732**, Parent PID: **5708**

General

Target ID:	3
Start time:	21:37:38
Start date:	15/05/2022
Path:	C:\ProgramData\windowupdate.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\windowupdate.exe
Imagebase:	0xd30000
File size:	2054656 bytes
MD5 hash:	35ED3FE203FABDE1B0D353815F9A273B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.310084355.0000000001080000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.310084355.0000000001080000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.310084355.0000000001080000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.310084355.0000000001080000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.525655922.00000000038E4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000002.525655922.00000000038E4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.310491730.00000000010BA000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.310491730.00000000010BA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.310491730.00000000010BA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.310491730.00000000010BA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000002.525427546.0000000002ED0000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000002.525427546.0000000002ED0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.525427546.0000000002ED0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000002.525427546.0000000002ED0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.310518053.0000000001080000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.310518053.0000000001080000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.310053824.00000000010A6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.310053824.00000000010A6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.310053824.00000000010A6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.310053824.00000000010A6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.310397605.00000000010A6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.310397605.00000000010A6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.310397605.00000000010A6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.310397605.00000000010A6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000002.525763010.0000000003A1F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000002.525763010.0000000003A1F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 17%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38E360F	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	38D2E05	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft Vision\15-05-2022_21.37.58	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	38D8932	CreateFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\windowupdate.exe	unknown	2054656	success or wait	1	38E1E78	ReadFile
C:\ProgramData\windowupdate.exe	unknown	2054656	success or wait	1	38E1E78	ReadFile
C:\Windows\SysWOW64\user32.dll	unknown	1626536	success or wait	1	38E1E78	ReadFile

Analysis Process: cmd.exe PID: 6080, Parent PID: 3968

General

Target ID:	6
Start time:	21:37:50
Start date:	15/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat" "
Imagebase:	0x7ff670f90000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	unknown	8191	success or wait	1	7FF670F9F404	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	unknown	8191	end of file	1	7FF670F9F404	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat:start	unknown	59	success or wait	1	7FF670F93977	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	unknown	8191	end of file	1	7FF670F9F404	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	unknown	8191	end of file	1	7FF670F9F404	ReadFile

Analysis Process: conhost.exe PID: 2460, Parent PID: 6080

General

Target ID:	8
Start time:	21:37:50
Start date:	15/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WMIC.exe PID: 5596, Parent PID: 6080

General

Target ID:	9
Start time:	21:37:51
Start date:	15/05/2022
Path:	C:\Windows\System32\wbem\WMIC.exe

Wow64 process (32bit):	false
Commandline:	wmic process call create "'C:\ProgramData:ApplicationData'"
Imagebase:	0x7ff630f20000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

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
\Device\ConDrv	38	38	4d 65 74 68 6f 64 20 65 78 65 63 75 74 69 6f 6e 20 73 75 63 63 65 73 73 66 75 6c 2e 0d 0d 0a 4f 75 74 20 50 61 72	Method execution successful.Out Par	success or wait	1	7FF630F5925F	fprintf
\Device\ConDrv	69	31	4f 75 74 20 50 61 72 61 6d 65 74 65 72 73 3a 0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f 5f	Out Parameters:instance of __	success or wait	1	7FF630F5925F	fprintf
\Device\ConDrv	84	15	0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f	instance of _	success or wait	1	7FF630F5925F	fprintf
\Device\ConDrv	138	54	0d 0a		success or wait	1	7FF630F5925F	fprintf
\Device\ConDrv	140	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF630F591F1	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **316**, Parent PID: **5732**

General

Target ID:	13
Start time:	21:37:55
Start date:	15/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x9b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: cmd.exe PID: **1636**, Parent PID: **5732**

General

Target ID:	14
Start time:	21:37:55
Start date:	15/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0xc20000
File size:	232960 bytes

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\windowupdate.exe	unknown	2054656	success or wait	1	32B026F	ReadFile

Analysis Process: conhost.exe PID: **4240**, Parent PID: **316**

General

Target ID:	15
Start time:	21:37:55
Start date:	15/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **3116**, Parent PID: **1636**

General

Target ID:	16
Start time:	21:37:56
Start date:	15/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: WmiPrvSE.exe PID: **1824**, Parent PID: **756**

General

Target ID:	18
Start time:	21:38:18
Start date:	15/05/2022
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff674600000
File size:	488448 bytes
MD5 hash:	A782A4ED336750D10B3CAF776AFE8E70
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly