ID: 764033
Sample Name: DQxttu2Qrr.exe
Cookbook: default.jbs
Time: 10:37:13
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

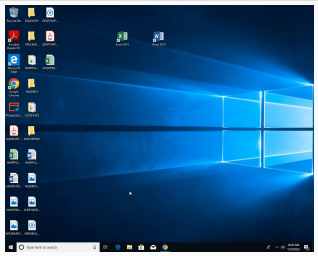
Windows Analysis Report

DQxttu2Qrr.exe

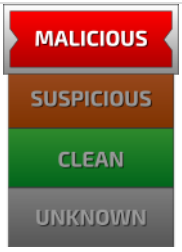
Overview

General Information

Sample Name:	DQxttu2Qrr.exe
Analysis ID:	764033
MD5:	7434b42e113802.
SHA1:	a2dea715e33a86.
SHA256:	9922432bfa7768..
Tags:	32 ArkeiStealer exe trojan
Infos:	



Detection



Amadey, Laplas Clipper, RedLine, SystemBC, Vidar

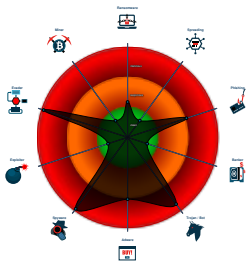
Score:

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

Signatures

- Yara detected RedLine Stealer
- Yara detected Amadeys stealer DLL
- Yara detected Laplas Clipper
- System process connects to networ…
- Yara detected SystemBC
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Vidar stealer
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…

Classification



Process Tree

- **System is w10x64**
- DQxttu2Qrr.exe (PID: 2508 cmdline: C:\Users\user\Desktop\DQxttu2Qrr.exe MD5: 7434B42E11380272961C92E061072E78)
  - 61312899942613011832.exe (PID: 5372 cmdline: "C:\ProgramData\61312899942613011832.exe" MD5: 2239A58CC93FD94DC2806CE7F6AF0A0B)
    - gntuud.exe (PID: 5780 cmdline: "C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe" MD5: 2239A58CC93FD94DC2806CE7F6AF0A0B)
      - schtasks.exe (PID: 5908 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN gntuud.exe /TR "C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 5920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5928 cmdline: "C:\Windows\System32\cmd.exe" /k echo Y|CACLS "gntuud.exe" /P "user:N"&&CACLS "gntuud.exe" /P "user:R" /E&&echo Y|CACLS "..\03bd543fce" /P "user:N"&&CACLS "..\03bd543fce" /P "user:R" /E&&Exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5996 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cacls.exe (PID: 6004 cmdline: CACLS "gntuud.exe" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
        - cacls.exe (PID: 6024 cmdline: CACLS "gntuud.exe" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
        - cmd.exe (PID: 6064 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cacls.exe (PID: 6076 cmdline: CACLS "..\03bd543fce" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
        - cacls.exe (PID: 6096 cmdline: CACLS "..\03bd543fce" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
      - rundll32.exe (PID: 6128 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll, Main MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - Emit64.exe (PID: 3920 cmdline: "C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe" MD5: 7A5155B804E592D83F8319CBDB27E164)
        - powershell.exe (PID: 3044 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe <#qgoyddbo#> IF((New-Object Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) { IF([System.Environment]::OSVersion.Version -lt [System.Version]"6.2") { schtasks /create /f /sc onlogon /rl highest /tn 'RtkAudUService64.exe' /tr '"C:\Users\user\Locktime\RtkAudUService64.exe"' } Else { Register-ScheduledTask -Action (New-ScheduledTaskAction -Execute 'C:\Users\user\Locktime\RtkAudUService64.exe') -Trigger (New-ScheduledTaskTrigger -AtLogOn) -Settings (New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -DisallowHardTerminate -DontStopIfGoingOnBatteries -DontStopOnIdleEnd -ExecutionTimeLimit (New-TimeSpan -Days 1000)) -TaskName 'RtkAudUService64.exe' -RunLevel 'Highest' -Force; } } Else { reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "RtkAudUService64.exe" /t REG_SZ /f /d 'C:\Users\user\Locktime\RtkAudUService64.exe' } MD5: 95000560239032BC68B4C2FDFCDEF913)
          - conhost.exe (PID: 5248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - avicapn32.exe (PID: 1112 cmdline: "C:\Users\user\1000018002\avicapn32.exe" MD5: 0F6EF96C5E687631EF27F1DCD1AFE7B4)
      - rundll32.exe (PID: 2820 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\1000019012\syncfiles.dll, rundll MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - umciavi64.exe (PID: 68 cmdline: "C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe" MD5: 8F727EA574C46E3FD8901335A6548285)
  - cmd.exe (PID: 5596 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "C:\Users\user\Desktop\DQxttu2Qrr.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5636 cmdline: timeout /t 6 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- gntuud.exe (PID: 4948 cmdline: C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe MD5: 2239A58CC93FD94DC2806CE7F6AF0A0B)

- cmd.exe (PID: 1500 cmdline: C:\Windows\System32\cmd.exe /c sc stop UsoSvc & sc stop WaaSMedicSvc & sc stop wuauserv & sc stop bits & sc stop dosvc & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\UsoSvc" /f & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\WaaSMedicSvc" /f & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\wuauserv" /f & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\bits" /f & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\dosvc" /f MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 3076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 5040 cmdline: sc stop UsoSvc MD5: D79784553A9410D15E04766AAAB77CD6)
  - sc.exe (PID: 3400 cmdline: sc stop WaaSMedicSvc MD5: D79784553A9410D15E04766AAAB77CD6)
  - sc.exe (PID: 4616 cmdline: sc stop wuauserv MD5: D79784553A9410D15E04766AAAB77CD6)
  - sc.exe (PID: 5488 cmdline: sc stop bits MD5: D79784553A9410D15E04766AAAB77CD6)
  - sc.exe (PID: 5224 cmdline: sc stop dosvc MD5: D79784553A9410D15E04766AAAB77CD6)
  - reg.exe (PID: 5848 cmdline: reg delete "HKLM\SYSTEM\CurrentControlSet\Services\UsoSvc" /f MD5: E3DACF0B31841FA02064B4457D44B357)
  - reg.exe (PID: 5772 cmdline: reg delete "HKLM\SYSTEM\CurrentControlSet\Services\WaaSMedicSvc" /f MD5: E3DACF0B31841FA02064B4457D44B357)
  - reg.exe (PID: 4864 cmdline: reg delete "HKLM\SYSTEM\CurrentControlSet\Services\wuauserv" /f MD5: E3DACF0B31841FA02064B4457D44B357)
  - reg.exe (PID: 1948 cmdline: reg delete "HKLM\SYSTEM\CurrentControlSet\Services\bits" /f MD5: E3DACF0B31841FA02064B4457D44B357)
  - reg.exe (PID: 5344 cmdline: reg delete "HKLM\SYSTEM\CurrentControlSet\Services\dosvc" /f MD5: E3DACF0B31841FA02064B4457D44B357)
- cmd.exe (PID: 2436 cmdline: C:\Windows\System32\cmd.exe /c powercfg /x -hibernate-timeout-ac 0 & powercfg /x -hibernate-timeout-dc 0 & powercfg /x -standby-timeout-ac 0 & powercfg /x -standby-timeout-dc 0 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5192 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powercfg.exe (PID: 1340 cmdline: powercfg /x -hibernate-timeout-ac 0 MD5: 7C749DC22FCB1ED42A87AFA986B720F5)
  - powercfg.exe (PID: 3508 cmdline: powercfg /x -hibernate-timeout-dc 0 MD5: 7C749DC22FCB1ED42A87AFA986B720F5)
  - powercfg.exe (PID: 5604 cmdline: powercfg /x -standby-timeout-ac 0 MD5: 7C749DC22FCB1ED42A87AFA986B720F5)
  - powercfg.exe (PID: 5836 cmdline: powercfg /x -standby-timeout-dc 0 MD5: 7C749DC22FCB1ED42A87AFA986B720F5)
- **cleanup**

Malware Configuration

Threatname: Amadey


```
{
  "C2 url": "85.209.135.109/jg94cVd30f/index.php",
  "Version": "3.50"
}
```


Threatname: Vidar


```
{
  "C2 url": [
    "http://65.21.119.56:80",
    "https://t.me/vmt001"
  ],
  "Botnet": "1760",
  "Version": "56.1"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\library[1].bin	SUSP_Two_Byte_XOR_PE_And_MZ	Look for 2 byte xor of a PE starting at offset 0	Wesley Shields <wxs@atarininja.org>	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\library[1].bin	SUSP_Four_Byte_XOR_PE_And_MZ	Look for 4 byte xor of a PE starting at offset 0	Wesley Shields <wxs@atarininja.org>	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\library[1].bin	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x4e:$xo1: \x8A\xB6\xB7\xAD\xFE\xAE\xAC\xB1\xB9\xAC\xBF\xB3\xFE\xBD\xBF\xB0\xB0\xB1\xAA\xFE\xBC\xBB\xFE\xAC\xAB\xB0\xFE\xB7\xB0\xFE\x9A\x91\x8D\xFE\xB3\xB1\xBA\xBB
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\umciavi32[1].exe	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
C:\Users\user\AppData\Roaming\1000021000\umciavi32.exe	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	

Click to see the 2 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000002.762181339.00000000003D1000.00000020.00000001.01000000.00000007.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000000.00000002.300367960.00000000010C5000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000031.00000002.656321722.000000000F230000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000031.00000002.656321722.000000000F230000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000031.00000003.546951720.000000000F0D2000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
49.3.umciavi64.exe.f0d0000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x4ad71:$s1: \x10\x0C\x0C\x08BWW • 0x4af3a:$s1: %99=wbb • 0x4d1e2:$s1: http:// • 0x4d3b1:$s1: +773yll • 0x4e274:$s1: \xEB\xF7\xF7\xF3\xB9\xAC\xAC • 0x88a55:$s1: \xA5\xB9\xB9\xBD\xF7\xE2\xE2 • 0x4ad7e:$s2: \x10\x0C\x0C\x08\x0BBWW • 0x4af47:$s2: %99=>wbb • 0x4d1ef:$s2: https:// • 0x4d3be:$s2: +7730yll • 0x51e96:$s2: ~bbfe,99 • 0x5225b:$s2: \x80\x9C\x9C\x98\x9B\xD2\xC7\xC7 • 0x79818:$s2: \x07\x1B\x1B\x1F\x1CU@@ • 0x798c5:$s2: \xB1\xAD\xAD\xA9\xAA\xE3\xF6\xF6 • 0x89534:$s2: \x1A\x06\x06\x02\x01H]] • 0x4d1e2:$f1: http:// • 0x4d1ef:$f2: https://
49.3.umciavi64.exe.f0d0000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
49.3.umciavi64.exe.f0d0000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
49.3.umciavi64.exe.f0d0000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
49.3.umciavi64.exe.f0d0000.0.unpack	MALWARE_Win_Arechclient2	Detects Arechclient2 RAT	ditekSHen	• 0x9905a:$s14: keybd_event • 0x9e480:$v1_1: grabber@ • 0x9688b:$v1_2: <BrowserProfile>k__ • 0x9798a:$v1_3: <SystemHardwares>k__ • 0x97a49:$v1_5: <ScannedWallets>k__ • 0x97ad9:$v1_6: <DicrFiles>k__ • 0x97ab5:$v1_7: <MessageClientFiles>k__ • 0x97e7f:$v1_8: <ScanBrowsers>k__BackingField • 0x97ed1:$v1_8: <ScanWallets>k__BackingField • 0x97eee:$v1_8: <ScanScreen>k__BackingField • 0x97f28:$v1_8: <ScanVPN>k__BackingField • 0x8ae5a:$v1_9: displayName[AString-ZaString-z\d]{2String4}\.[String\w-]{String6}\.[\wString-]{2String7}Local Extension Settingshost • 0x8a666:$v1_10: \sitemanager.xml MB or SELECT * FROM Cookiesconfig

Click to see the 18 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking

System process connects to network (likely due to code injection or exploit)

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

PE file contains section with special chars

Uses powercfg.exe to modify the power settings

Persistence and Installation Behavior

Uses cmd line tools excessively to alter registry or file data

Boot Survival

Creates multiple autostart registry keys

Uses schtasks.exe or at.exe to add and modify task schedules

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Overwrites code with function prologues

Self deletion via cmd or bat file

Found hidden mapped module (file has been removed from disk)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

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

Tries to evade analysis by execution special instruction (VM detection)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging

Tries to detect debuggers (CloseHandle check)

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

.NET source code references suspicious native API functions

Modifies the hosts file

Modifies the context of a thread in another process (thread injection)

Lowering of HIPS / PFW / Operating System Security Settings

Modifies power options to not sleep / hibernate

Modifies the hosts file

Stealing of Sensitive Information

Yara detected RedLine Stealer

Yara detected Amadeys stealer DLL

Yara detected Laplas Clipper

Yara detected SystemBC

Yara detected Vidar stealer

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

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

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality

Yara detected RedLine Stealer

Yara detected SystemBC

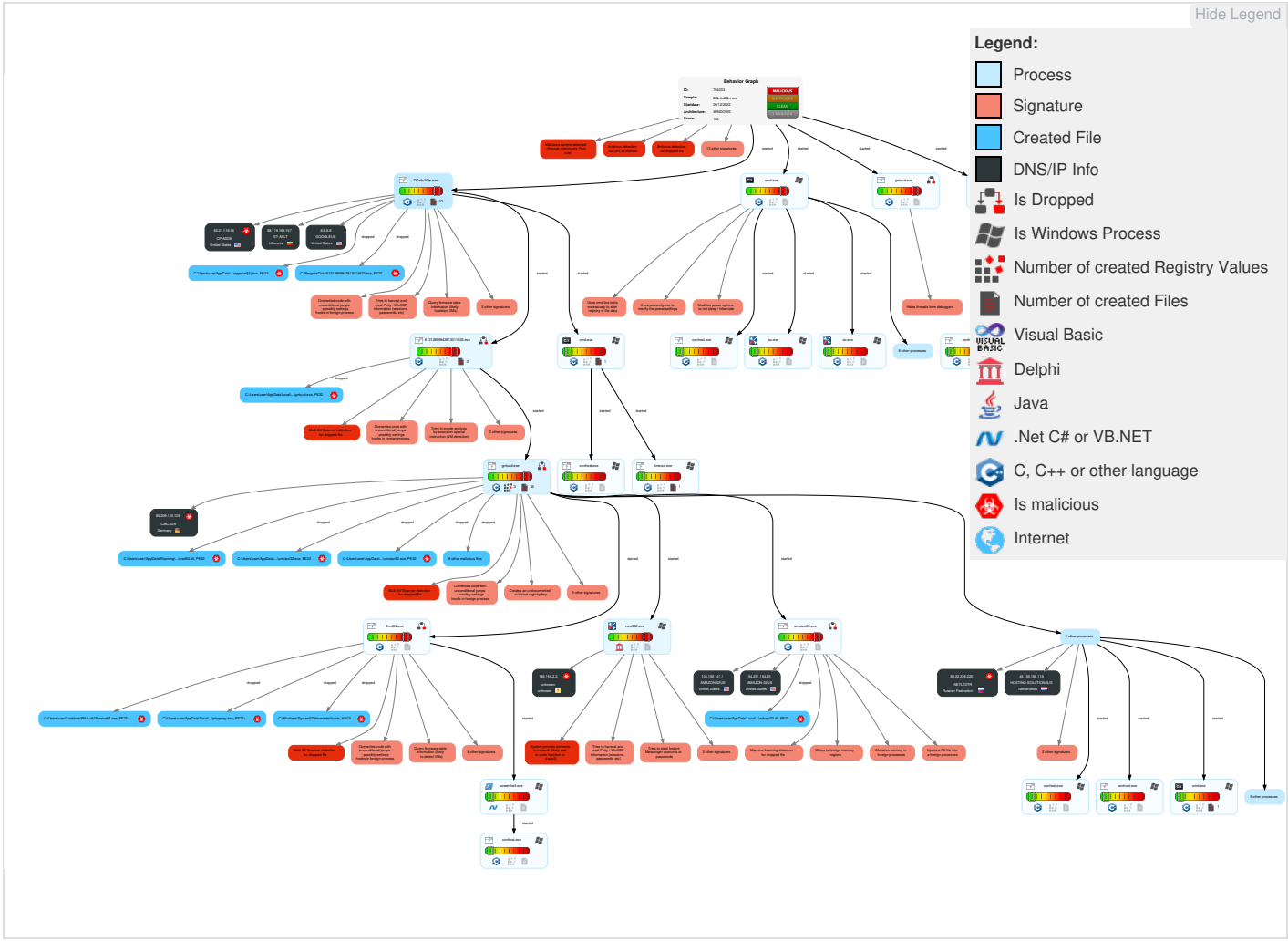
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 1 Command and Scripting Interpreter	1 Windows Service	1 Windows Service	2 Obfuscated Files or Information	1 Credential API Hooking	2 File and Directory Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	6 1 1 Process Injection	3 Software Packing	1 Input Capture	2 3 5 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Service Execution	2 1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 DLL Side-Loading	2 Credentials in Registry	7 3 1 Security Software Discovery	Distributed Component Object Model	1 Credential API Hooking	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	1 Services File Permissions Weakness	2 1 Registry Run Keys / Startup Folder	1 File Deletion	1 Credentials In Files	1 1 Process Discovery	SSH	1 Input Capture	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	1 Services File Permissions Weakness	1 Masquerading	Cached Domain Credentials	2 4 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Modify Registry	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 4 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	6 1 1 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Services File Permissions Weakness	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

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
DQxttu2Qrr.exe	36%	ReversingLabs	Win32.Infostealer.Bandra	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\jekppnay.tmp	100%	Avira	HEUR/AGEN.1236196	
C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\umciavi64[1].exe	100%	Joe Sandbox ML		
C:\Users\user\Locktime\RtkAudUService64.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\jekppnay.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\advapi32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Emit64[1].exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\ProgramData\6131289994261301 1832.exe	35%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\1000018002\avicapn32.exe	15%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\1000019012\syncfiles.dll	23%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\syncfiles[1].dll	23%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\avicapn32[1].exe	15%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\umciavi64[1].exe	18%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Emit64[1].exe	27%	ReversingLabs	Win64.Trojan.Generic	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	12%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\nppshell[1].exe	35%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe	35%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe	27%	ReversingLabs	Win64.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\advapi32.dll	20%	ReversingLabs	Win32.Spyware.RedLine	
C:\Users\user\AppData\Local\Temp\jekppnay.tmp	81%	ReversingLabs	ByteCode-MSIL.Trojan.Tedy	
C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe	18%	ReversingLabs		
C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll	12%	ReversingLabs		
C:\Users\user\Locktime\RtkAudUService64.exe	27%	ReversingLabs	Win64.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.DQxttu2Qrr.exe.1090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
49.3.umciavi64.exe.f0d0000.1.unpack	100%	Avira	HEUR/AGEN.1235675		Download File
0.0.DQxttu2Qrr.exe.1090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
49.3.umciavi64.exe.f0d0000.0.unpack	100%	Avira	HEUR/AGEN.1235675		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://65.21.119.56:80	100%	Avira URL Cloud	malware	
http://https://d301sr5gafysq2.cloudfront.net;	0%	Avira URL Cloud	safe	
http://ripple-wells-2022.net/	0%	Avira URL Cloud	safe	
http://65.21.119.56:80https://t.me/vmt001hello0;open_open	0%	Avira URL Cloud	safe	
http://65.21.119.56:80/update.zip	100%	Avira URL Cloud	malware	
http://cjdlifvn3qkbi0ymi0ma.wclwox4jcqzsnqbjvs/	0%	Avira URL Cloud	safe	
http://cjdlifvn3qkbi0ymi0ma.wclwox4jcqzsnqbjvs/)a	0%	Avira URL Cloud	safe	
85.209.135.109/jg94cVd30f/index.php	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://65.21.119.56:80/update.zipb0dfc5b548762778904926-d06ed635-68f6-4e9a-955c-90ce-806e6f6e6963	100%	Avira URL Cloud	malware	
http://cjDliFVN3QKbi0ymi0MA.WclWOx4jCqZsNQbjvsAivMLJa9uT5DhrasATByTHQ5iENK14UsJkLrDsnRarngdZ7r0MiULb	0%	Avira URL Cloud	safe	
http://https://ion=v4.5	0%	Avira URL Cloud	safe	
http://167.235.150.8:80	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://65.21.119.56:80	true	• Avira URL Cloud: malware	unknown
85.209.135.109/jg94cVd30f/index.php	true	• Avira URL Cloud: safe	low
http://https://t.me/vmt001	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/minor.bin	umciavi64.exe, 00000031.00000003.627649701.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://cjdlifvn3qkbi0ymi0ma.wclwox4jcqzsnqbjvs/)a	umciavi64.exe, 00000031.00000003.629628004.0000000000966000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000002.641706708.0000000000966000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	6131289994261301183 2.exe, 00000004.00000003.307229091.0000000001061000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe	false	• URL Reputation: safe	unknown
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/minor.bin8	umciavi64.exe, 00000031.00000002.643481075.00000000009BA000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.632274574.00000000009BA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bbuseruploads.s3.amazonaws.com/f3ef24fc-08b2-408a-a2c5-1fad12572ea6/downloads/b803c041-f8b5-	umciavi64.exe, 00000031.00000003.627649701.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000020.00000002.707622809.000001A0A439D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ripple-wells-2022.net/	gntuud.exe, 0000000D.00000003.367330103.00000000016F0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/intl/en_uk/chrome/https://www.google.com/intl/en_uk/chrome/https://www.google	DQxttu2Qrr.exe, 00000000.00000003.264721352.0000000027ACD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://steamcommunity.com/profiles/76561199441933804	umciavi64.exe, 00000031.00000003.619550432.000000000F2F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/minor.binR	umciavi64.exe, 00000031.00000002.643481075.00000000009BA000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.632274574.00000000009BA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://cjdlifvn3qkbi0ymi0ma.wclwox4jcqzsnqbjvs/	umciavi64.exe, 00000031.00000003.629628004.0000000000966000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000002.641706708.0000000000966000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://65.21.119.56:80/update.zip	DQxttu2Qrr.exe, 00000000.00000002.298542710.00000000004FD000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

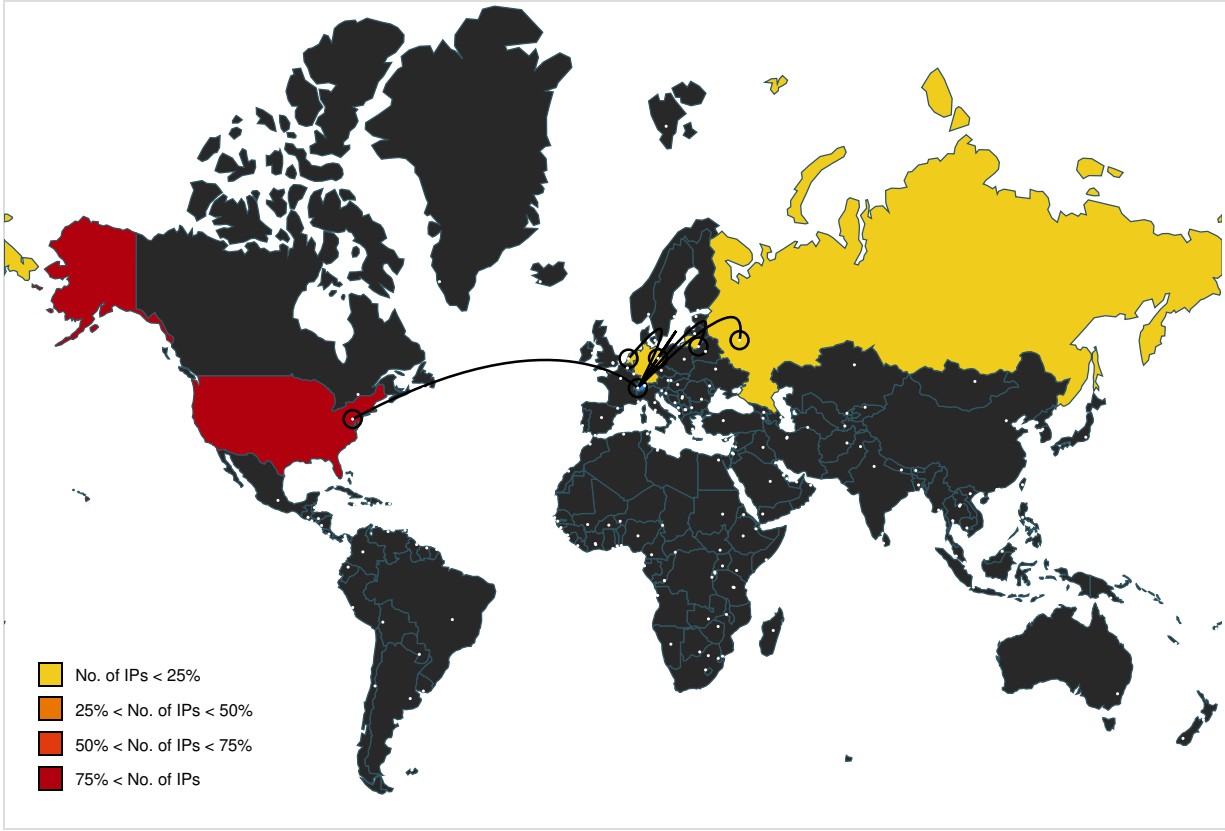
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/answer/6315198?product=	DQxttu2Qrr.exe, 00000000.00000002.328642046.0000000027CBE000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe, 00000000.00000003.264518594.0000000027ACD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/library.bin	umciavi64.exe, 00000031.00000002.641706708.0000000000966000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.562128012.0000000000A19000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.631988058.00000000009B1000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000002.642766425.00000000009B1000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.554465568.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://d301sr5gafysq2.cloudfront.net;	umciavi64.exe, 00000031.00000003.554465568.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://support.google.com/chrome/answer/111996?visit_id=637962485686793996-3320600880&p=update_erro	DQxttu2Qrr.exe, 00000000.00000002.328642046.0000000027CBE000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe, 00000000.00000003.264518594.0000000027ACD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/intl/en_uk/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrows	DQxttu2Qrr.exe, 00000000.00000002.328642046.0000000027CBE000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe, 00000000.00000003.264518594.0000000027ACD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/resource.bin0c9c7142b75e/library.bin	umciavi64.exe, 00000031.00000003.567296026.00000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.591831541.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/resource.binn	umciavi64.exe, 00000031.00000003.567296026.00000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.591831541.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/intl/en_uk/chrome/	DQxttu2Qrr.exe, 00000000.00000002.328859576.0000000027DCD000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe, 00000000.00000002.328642046.0000000027CBE000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe, 00000000.00000003.264518594.0000000027ACD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/resource.bint	umciavi64.exe, 00000031.00000002.643481075.00000000009BA000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.632274574.00000000009BA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/ww	umciavi64.exe, 00000031.00000003.629628004.0000000000966000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000002.641706708.0000000000966000.00000004.00000020.00020000.00000000.sdmp	false		high
http://65.21.119.56:80/update.zipb0dfc5b548762778904926-d06ed635-68f6-4e9a-955c-90ce-806e6f6e6963	DQxttu2Qrr.exe, 00000000.00000002.298542710.00000000004FD000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://contoso.com/	powershell.exe, 00000020.00000002.707622809.000001A0A439D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000020.00000002.707622809.000001A0A439D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://bbuseruploads.s3.amazonaws.com/f3ef24fc-08b2-408a-a2c5-1fad12572ea6/downloads/b97f81fe-0ba4-	umciavi64.exe, 00000031.00000003.627649701.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/resource.bin	umciavi64.exe, 00000031.00000003.6322745 74.00000000009BA000.00000004.00000020.00 020000.00000000.sdmp, umciavi64.exe, 000 00031.00000003.569146497.0000000000A1A00 0.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.568886955.000 0000000A1A000.00000004.00000020.00020000 .00000000.sdmp, umciavi64.exe, 00000031. 00000003.627649701.00000000009C8000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/minor.bin6	umciavi64.exe, 00000031.00000002.6439574 50.00000000009CF000.00000004.00000020.00 020000.00000000.sdmp, umciavi64.exe, 000 00031.00000003.627649701.00000000009C800 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome?p=update_error	DQxttu2Qrr.exe, 00000000.00000002.328642 046.0000000027CBE000.00000004.00000800.0 0020000.00000000.sdmp, DQxttu2Qrr.exe, 0 0000000.00000003.264518594.0000000027ACD 000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000020.00000002.656197 895.000001A094341000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://65.21.119.56:80https://t.me/vmt001hello0;open_open	DQxttu2Qrr.exe, 00000000.00000002.300367 960.00000000010C5000.00000002.00000001.0 1000000.00000003.sdmp	false	• Avira URL Cloud: safe	low
http://https://bbuseruploads.s3.amazonaws.com/E	umciavi64.exe, 00000031.00000003.5620725 36.00000000009D8000.00000004.00000020.00 020000.00000000.sdmp, umciavi64.exe, 000 00031.00000002.643957450.00000000009CF00 0.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.567296026.000 00000009C8000.00000004.00000020.00020000 .00000000.sdmp, umciavi64.exe, 00000031. 00000003.591831541.00000000009C8000.0000 0004.00000020.00020000.00000000.sdmp, um ciavi64.exe, 00000031.00000003.627649701 .00000000009C8000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://bbuseruploads.s3.amazonaws.com/H	umciavi64.exe, 00000031.00000003.5620725 36.00000000009D8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/resource.bind	umciavi64.exe, 00000031.00000003.5672960 26.00000000009C8000.00000004.00000020.00 020000.00000000.sdmp, umciavi64.exe, 000 00031.00000003.591831541.00000000009C800 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sqlite.org/copyright.html.	DQxttu2Qrr.exe, 00000000.00000002.325985 352.0000000027895000.00000004.00000800.0 0020000.00000000.sdmp, DQxttu2Qrr.exe, 0 0000000.00000002.331524675.0000000061ED3 000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://bbuseruploads.s3.amazonaws.com/l	umciavi64.exe, 00000031.00000003.5620725 36.00000000009D8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://bitbucket.org/	umciavi64.exe, 00000031.00000003.6276497 01.00000000009C8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000020.00000002.707622 809.000001A0A439D000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	6131289994261301183 2.exe, 00000004.00000 003.307229091.0000000001061000.00000004. 00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe	false	• URL Reputation: safe	unknown
http://https://t.me/dishastahttps://steamcommunity.com/profiles/76561199441933804167.235.150.8:80dis	umciavi64.exe, 00000031.00000003.6195504 32.000000000F2F1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://www.google.com/search?q=chrome&oq=chrome&aqs=chrome..69i57j0j5l3j69i60l3.2663j0j4&sourceid=c	DQxttu2Qrr.exe, 00000000.00000002.328642 046.0000000027CBE000.00000004.00000800.0 0020000.00000000.sdmp, DQxttu2Qrr.exe, 0 0000000.00000003.264518594.0000000027ACD 000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000020.00000002.661457 199.000001A094548000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000020.00000002.661457 199.000001A094548000.00000004.00000800.0 0020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000020.00000002.661457199.000001A094548000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://bbuseruploads.s3.amazonaws.com/f3ef24fc-08b2-408a-a2c5-1fad12572ea6/down.	umciavi64.exe, 00000031.00000003.561824002.0000000000A19000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.562128012.0000000000A19000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000020.00000003.420288387.000001A095FA4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://bbuseruploads.s3.amazonaws.com/f3ef24fc-08b2-408a-a2c5-1fad12572ea6/downloads/cba79466-746d-	umciavi64.exe, 00000031.00000003.627649701.0000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://web-security-reports.services.atlassian.com/csp-report/bb-website	umciavi64.exe, 00000031.00000003.567296026.0000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.569146497.0000000000A1A000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.568886955.0000000000A1A000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.554465568.0000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://cjDliFVN3QKbi0ymi0MA.WclWOx4jCqZsNQbjvsAivMLJa9uT5DhrasATByTHQ5iENK14UsJkLrDsnRarngdZ7r0MiULb	umciavi64.exe, 00000031.00000002.649017901.00000000029E3000.00000040.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000020.00000002.707622809.000001A0A439D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://bitbucket.org/versal	umciavi64.exe, 00000031.00000002.643957450.0000000009CF000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.627649701.0000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000020.00000002.661457199.000001A094548000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/installer/?product=	DQxttu2Qrr.exe, 00000000.00000002.328642046.0000000027CBE000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe, 00000000.00000003.264518594.0000000027ACD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://167.235.150.8:80	umciavi64.exe, 00000031.00000003.619550432.000000000F2F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/resource.bin8	umciavi64.exe, 00000031.00000003.567296026.0000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	6131289994261301183 2.exe, 00000004.00000003.307229091.0000000001061000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe	false	• URL Reputation: safe	unknown
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/library.binIua2gnOxsYQNjWglYDZ3357MMJTmqF	umciavi64.exe, 00000031.00000002.649017901.00000000029E3000.00000040.00000800.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597	umciavi64.exe, 00000031.00000003.629628004.0000000000966000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000002.641706708.0000000000966000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ion=v4.5	powershell.exe, 00000020.00000002.719705380.000001A0AC974000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.zlib.net/D	avicapn32.exe, 0000001B.00000002.857905860.00000000017DE000.00000002.00000001.01000000.0000000B.sdmp	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	6131289994261301183 2.exe, 00000004.00000003.307229091.0000000001061000.00000004.00000800.00020000.00000000.sdmp, DQxttu2Qrr.exe	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000020.00000002.661457199.000001A094548000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bitbucket.org/D	umciavi64.exe, 00000031.00000002.643957450.00000000009CF000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.567296026.00000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.591831541.00000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.627649701.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/minor.binin	umciavi64.exe, 00000031.00000002.643481075.00000000009BA000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.632274574.00000000009BA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://aui-cdn.atlassian.com	umciavi64.exe, 00000031.00000003.567296026.00000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.569146497.0000000000A1A000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.568886955.0000000000A1A000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.554465568.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bbuseruploads.s3.amazonaws.com/	umciavi64.exe, 00000031.00000003.562072536.00000000009D8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000002.643957450.00000000009CF000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.567296026.00000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.591831541.00000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.554465568.00000000009C8000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.627649701.00000000009C8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://bitbucket.org/alfolod79597/advancedapi32/downloads/minor.binl	umciavi64.exe, 00000031.00000002.643481075.00000000009BA000.00000004.00000020.00020000.00000000.sdmp, umciavi64.exe, 00000031.00000003.632274574.00000000009BA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/dishasta	umciavi64.exe, 00000031.00000003.619550432.000000000F2F1000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
65.21.119.56	unknown	United States		199592	CP-ASDE	true
89.22.236.225	unknown	Russian Federation		197328	INETLTDTR	true
104.192.141.1	unknown	United States		16509	AMAZON-02US	false
45.159.188.118	unknown	Netherlands		14576	HOSTING-SOLUTIONSUS	false
54.231.164.65	unknown	United States		16509	AMAZON-02US	false
88.119.169.157	unknown	Lithuania		61272	IST-ASLT	false
85.209.135.109	unknown	Germany		33657	CMCSUS	true

Private

IP
192.168.2.3

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764033
Start date and time:	2022-12-09 10:37:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DQxttu2Qrr.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	57
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.adwa.spyw.evad.winEXE@83/38@0/9
EGA Information:	• Successful, ratio: 25%
HDC Information:	• Successful, ratio: 4.8% (good quality ratio 3.2%) • Quality average: 42.8% • Quality standard deviation: 35.7%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- Exclude process from analysis (whitelisted): MpCmdRun.exe, Conhost.exe, rundll32.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Execution Graph export aborted for target Emit64.exe, PID 3920 because there are no executed function
- Execution Graph export aborted for target avicapn32.exe, PID 1112 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- 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 getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: DQxttu2Qrr.exe

Simulations

Behavior and APIs

Time	Type	Description
10:38:51	Task Scheduler	Run new task: gntuud.exe path: C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
10:38:52	API Interceptor	1283x Sleep call for process: gntuud.exe modified
10:39:15	API Interceptor	1x Sleep call for process: Emit64.exe modified
10:39:22	API Interceptor	36x Sleep call for process: powershell.exe modified
10:39:25	API Interceptor	1x Sleep call for process: rundll32.exe modified
10:39:42	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run umciavi64.exe C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe
10:39:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run umciavi32.exe C:\Users\user\AppData\Roaming\1000021000\umciavi32.exe
10:40:01	Autostart	Run: C:\Users\user\AppData\Local\Temp\03bd543fce\\gntuud.exe
10:40:16	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run umciavi64.exe C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe
10:40:25	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run umciavi32.exe C:\Users\user\AppData\Roaming\1000021000\umciavi32.exe
10:41:03	Task Scheduler	Run new task: RtkAudUService64.exe path: C:\Users\user\Locktime\RtkAudUService64.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\111642860579162299991747962

Process:	C:\Users\user\Desktop\DQxttu2Qrr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\ProgramData\116934309704013069444944184

Process:	C:\Users\user\Desktop\DQxttu2Qrr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 7, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.7217007190866341
Encrypted:	false
SSDEEP:	384:kab+d5neKTnuRpHDiEwABBE3umab+QuJdi:kab+dVeK8iEZBBjmab+QuJdi
MD5:	FEF7F4B210100663DC7731400BAC534E
SHA1:	E3F17C46A2DB6861F22B3F4222B97DCB5EBBD47A
SHA-256:	E81118F5C967EA342A16BDEFB28919F8039E772F8BDCF4A65684E3F56D31EA0E
SHA-512:	6134CC2118FBADD137C4FC3204028B088C7E73A7B985A64D84C60ABD5B1DBFD0AA352C6DF199F43164FEC92378571B5FAC4F801E9AF7BE1DEA8FB6C3C799F 95
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\ProgramData\14765269315554389947119608

Process:	C:\Users\user\Desktop\DQxttu2Qrr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped

Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\ProgramData\17061304525933759500214796

Process:	C:\Users\user\Desktop\DQxttu2Qrr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\44571614278734644827034568

Process:	C:\Users\user\Desktop\DQxttu2Qrr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\48205952313381291261104955

Process:	C:\Users\user\Desktop\DQxttu2Qrr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 7, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.7217007190866341
Encrypted:	false
SSDEEP:	384:kab+d5neKTnuRpHDiEwABBE3umab+QuJdi:kab+dVeK8iEZBBjmab+QuJdi
MD5:	FEF7F4B210100663DC7731400BAC534E
SHA1:	E3F17C46A2DB6861F22B3F4222B97DCB5EBBD47A

SHA-256:	E81118F5C967EA342A16BDEFB28919F8039E772F8BDCF4A65684E3F56D31EA0E
SHA-512:	6134CC2118FBADD137C4FC3204028B088C7E73A7B985A64D84C60ABD5B1DBFD0AA352C6DF199F43164FEC92378571B5FAC4F801E9AF7BE1DEA8FB6C3C799F 95
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\ProgramData\61312899942613011832.exe

Process:	C:\Users\user\Desktop\DQxttu2Qrr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7732440
Entropy (8bit):	7.8779499305543865
Encrypted:	false
SSDEEP:	196608:U+rNR2F7EU+iE09OKsRk3PdM+i+8lHFL9AYS:/RWEU+1OP6+X+oYS
MD5:	2239A58CC93FD94DC2806CE7F6AF0A0B
SHA1:	F09EB7D69BC7440D3D45E14267236A78AC789FCB
SHA-256:	682ABD62B6E3C0E8CA57F079CD96F2D3848752EAF7002BDF57BFB512BD242811
SHA-512:	F77C16626A0E17FF79B95F9FDED6A365F913896C89BAF76D16BCC8706F3AD10A9476C7CBD3F235250B936171C6E958E145C402952506DC0E434A4F911C99FE0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....XH..6...6...6...5...6...3.a.6...2...6.(.2...6.(.5...6.(.3...6...7...6...7.\.6.f. ?...6.f.....6.f.4...6.Rich..6.....PE..L....6.c.....r.....FU.....@.....~.v...@.....p.....`..`c.....u.....P.....0E..p..... A..@.....A.h.....lB@dO\ih..... ..`Fh?jG[OJL.....@..@qNR5:WbSLD.....@...z?fd8ijJh.=..... ..`CV?7x >JO.....A.....@...EVjKc_MI.wo...A..xo..... ..`dT<:EHzj.....P.....o.....@..@@]topACL`c...`...\....o.....@..@..... .....

C:\Users\user\1000018002\avicapn32.exe

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	12684504
Entropy (8bit):	7.510645764082388
Encrypted:	false
SSDEEP:	196608:dwT9pIuAU3qr4DZDZWHvmwIHEQWiXkOSsCYSwD8Qtwi85lW:wv6YDWHvm3HznXk+C12t45lW
MD5:	0F6EF96C5E687631EF27F1DCD1AFE7B4
SHA1:	EA8AEEE11C243E3EACFA6753F708C20CBBA39AAC
SHA-256:	38381A42975028B181430A80D6009988D0D0CFA42493D3EFBBFB72D3ABE97648
SHA-512:	3AE1986071AFFFBED1978BE560D5159F563D699BE798E6AB6DC616A82104467B79EC872C891E11615D3793348730F311BCE3A63F1CE289BB8D7C73399C26C5C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_LaplasClipper, Description: Yara detected Laplas Clipper, Source: C:\Users\user\1000018002\avicapn32.exe, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#.....T.....`C...@..... ..@.....d....p...a.....v.....$.....8.....text...e.#.....#..... ..`.rdata...P....$..R....#.....@..@.data ....B...`C..L...FC.....@....idata.....I.....F.....@....n3DK0...m....I..n....F.....@..@.symtab.....0K.....H.....@.n3DK1...8B..@K..:B...H..... ..`.n3DK 2.....@.....@....n3DK3...E4.....F4..F..... ..`.reloc..$.....@..@.rsrc....a...p...b.....@..@..... .....

C:\Users\user\1000019012\syncfiles.dll

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7566544
Entropy (8bit):	7.976819466268135
Encrypted:	false
SSDEEP:	196608:l3ksPqmzcl+LG314Hujb7KgkYCbGNBmHTER:lUON+2HBb8
MD5:	0D079A931E42F554016DB36476E55BA7
SHA1:	D5F1AB52221019C746F1CC59A45CE18D0B817496
SHA-256:	EAD2C5AAF92FE07DB45B99587F586C7A45F92C67220CD8113A5D2E7BCB320798
SHA-512:	1496F1296DF89E1DA8780F175631E2551300A99E6C7EA43D2750653FDF6E7ED096FDEDD9F0D23B94190ECF418DA09CF9C9B6CAEE5821BA1C457F0294063BBC E

Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...8.ob.....!....."...@.....=XT.....@..... .....Ft...../..E...<.f.....^s.....0C.x.....*;>%1sXO.!..... ..`7rP!Ni:jE....@..... ..@..@bkE<E2?8P....P.....@...8*7`Joyqd.B..`..... ..`0Ys"'rSd.....0C.....@...nUPwRZiK.Es..@C..Fs..... ..`$u!6XeN&.....Ps..... ..@..@K)'tLNvc.....Vs.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\library[1].bin

Process:	C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe
File Type:	data
Category:	dropped
Size (bytes):	278528
Entropy (8bit):	6.627837746051646
Encrypted:	false
SSDEEP:	6144:Vi/iVF4UXV8iHHsOa2TVYZksfrJAUfYF7jzDquQ7OXmmMGQBpaSbics154GgLPEr:U/iVF4UXV8iHHsOa2RYZksfrJAUQF7jb
MD5:	85FD3919C3113C160EA76DBFCDB69E26
SHA1:	5189553FA48EDD0CCCD31169F11091FE48D28D42
SHA-256:	C7A90D3A3EE42F62540F02E6CAD282F8262D55BADA6D7977DFACD038408AB484
SHA-512:	D837D0B8DBCABBB05891A84356EF52936756B2E1CAAD065B37981C16467158DCBD586F8C07821ADD047AAAA656C0E8264C71429F046EA4924A37CEEA913954E
Malicious:	false
Yara Hits:	• Rule: SUSP_Two_Byte_XOR_PE_And_MZ, Description: Look for 2 byte xor of a PE starting at offset 0, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\library[1].bin, Author: Wesley Shields <wxs@atarininja.org> • Rule: SUSP_Four_Byte_XOR_PE_And_MZ, Description: Look for 4 byte xor of a PE starting at offset 0, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\library[1].bin, Author: Wesley Shields <wxs@atarininja.org> • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\library[1].bin, Author: Florian Roth
Preview:	.....d..j...f.....A.L.....>.....6.....J`.....*`..... .....j.....^...b.....~.....B.....j.....W;..]2.U..W.^U..W.ZU .....(]0.W...,q.]?.]'..J.^?.V.P]&..B...V.Q..V.p.=U.VW[.!!!..._^.Z....7....U[.!!!....].Z....7....U[.!!!...I[.Z....7....U[.!!!.s.YY.Zu...7....U[.!!!.B..R.Z....7....U[.!!!...P.Z....7....U[.!!!.RN.ZP...7....U[.!!!..O.Z....7....U[.!!!.$..L.Z....7....U[.!!!.[&L.Z....7....U[.!!!...M.Z....7....U[.!!!....K.Z....7....U[.!!!.D"]K.ZH...7....U[.!!!...dD.ZA...7....U[.!!!.d.E.Z#...7....U[.!!!.C..~.Z....7.. ..U[.!!!.._cz.Z....7....U[.!!!..az.Z....7....U[.!!!....z.Z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\syncfiles[1].dll

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7566544
Entropy (8bit):	7.976819466268135
Encrypted:	false
SSDEEP:	196608:l3ksPqmzcl+LG314Hujb7KgkYCbGNBmHTER:lUON+2HBb8
MD5:	0D079A931E42F554016DB36476E55BA7
SHA1:	D5F1AB52221019C746F1CC59A45CE18D0B817496
SHA-256:	EAD2C5AAF92FE07DB45B99587F586C7A45F92C67220CD8113A5D2E7BCB320798
SHA-512:	1496F1296DF89E1DA8780F175631E2551300A99E6C7EA43D2750653FDF6E7ED096FDEDD9F0D23B94190ECF418DA09CF9C9B6CAEE5821BA1C457F0294063BBCE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...8.ob.....!....."...@.....=XT.....@..... .....Ft...../..E...<.f.....^s.....0C.x.....*;>%1sXO.!..... ..`7rP!Ni:jE....@..... ..@..@bkE<E2?8P....P.....@...8*7`Joyqd.B..`..... ..`0Ys"'rSd.....0C.....@...nUPwRZiK.Es..@C..Fs..... ..`$u!6XeN&.....Ps..... ..@..@K)'tLNvc.....Vs.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\avicapn32[1].exe

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	12684504
Entropy (8bit):	7.510645764082388
Encrypted:	false
SSDEEP:	196608:dwT9pIuAU3qr4DZDZWHvmwIHEQWiXkOSsCYSwD8Qtwi85lW:wv6YDWHvm3HznXk+C12t45lW
MD5:	0F6EF96C5E687631EF27F1DCD1AFE7B4
SHA1:	EA8AEEE11C243E3EACFA6753F708C20CBBA39AAC

SHA-256:	38381A42975028B181430A80D6009988D0D0CFA42493D3EFBBFB72D3ABE97648
SHA-512:	3AE1986071AFFFBED1978BE560D5159F563D699BE798E6AB6DC616A82104467B79EC872C891E11615D3793348730F311BCE3A63F1CE289BB8D7C73399C26C5C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_LaplasClipper, Description: Yara detected Laplas Clipper, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\avicapn32[1].exe, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#.....T.....`C...@..... ..@.....d....p...a.....v.....$.....8.....text...e.#.....#..... ..`.rdata...P....$..R....#.....@..@.data ....B...`C..L...FC.....@....idata.....I.....F.....@....n3DK0...m....I..n....F.....@..@.symtab.....0K.....H.....@.n3DK1...8B..@K..:B...H..... ..`.n3DK 2.....@.....@....n3DK3...E4.....F4..F..... ..`.reloc..$.....@..@.rsrc....a...p...b.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\umciavi32[1].exe

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1678464
Entropy (8bit):	7.9507150099938295
Encrypted:	false
SSDEEP:	49152:20ldRpIqyIKbA+iRYknKnO3YnQI/vKXBs:2+RpaIKbdNkKnO3YnQI/vms
MD5:	B66347E9A4018F257A6BF1941B4A5D60
SHA1:	0F4A358AD14E441F74C634054D798E6BE2DA476D
SHA-256:	D74BF0394DE0AD2ADCFD7ECC96711BAC682F3749F8953701EEFC596B8C11DD36
SHA-512:	EAB7414A3D2ED2AAB80EB4452E8B30B6E7481E7CB48BDB986450196EA8695008F7B26D3EE423934A0D6B30650CCD3E50B64CC979723D9DF2DF31052875C046 5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\umciavi32[1].exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....NSBGANBRBZHTLGXNSXICJRIHFRNKTLYIZVLK QZWZZIPOYNKNILJIIOVPNXKJVVPH.....Xy..PE..L....^B*.....x.....@.....`.....@.....0.... .....Xy..(#.....#.....CODE.....w.....x..... ..`DATA..... ...|.....@...BSS.....E.....idata..... .....@....tls.....rdata.....@..P.reloc...#.....$.....@..P.rsrc.....0.....@..P.....P.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\resource[1].bin

Process:	C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe
File Type:	data
Category:	dropped
Size (bytes):	142689
Entropy (8bit):	**7.998723425236566**
Encrypted:	**true**
SSDEEP:	3072:Qcxgv1IIK1ilFlYZpomLYew9lly75DinozOhzTHHyw:c1IlvBwpFSQ75Df6RSw
MD5:	25B8AC2C67E40924ECAC2C69919D0F2B
SHA1:	717790EEB21A3CE77A5A04E50B295C5EA1B44CC5
SHA-256:	5D653986D4C2E30A79A8753F65D0A757DBFE3359990138C73BD6FDFBF12B7D77
SHA-512:	7EE498092B98DF442815FFE6F54B596BDB61480AAD4CBE1CF5EBC6C4DA94A3B5B15422F1E5453296A1C6F6082AE3A776399F7502756D3887878347F1AF34B4D
Malicious:	false
Preview:	p....AP.w{...V.Iv...9Ow.[.M.Q1.!....,.....{....L.3..Y.....i.?Cm.|ilZ.f ..m...!G.....j....;Y...U.]...N.:.8...5.z..%B.*N...>@..D..J...#j.Xdx.I.:$..BD..v..7.....I.1.H....2..+5...pi..."@'.$0"{. il.7....c.<~..@.#V)".U.6..-.....P.#..?.).K....?gST.mw..%v.j,.s....N.c.YO(.L/...R..O>...).5.&.....D.{R.(....>..".._.S..s./T....I.}.>..K2..y...`.p.&..n..:.c.K~..0.i?(.e.c$.=....D..1....RZ.}.5uS .I...ZE. ..M\.[Q..N...I&cz.#.`/.=(2.....g....$.j..e..{1BO-27.....`BO-27.....`BO-27.....`BO-27.....`BO-27.....`BO-27.....`BO-27.....`BO-27.....`BO-27.....`BO- 27.....`~q.....]s.Y9.y..c.N*>....]..W....+.....d.S4.....]..?wV..|...x.....pd..o.;$F.kiE.-.1<.....i.t.J....k...]....]...2.^,.....k..@..Z.rx.....6-'(...`..f-`.S.J.5.w..M.5..Y.{.;..q(..D.~&. .Wq.ri. .#'..6..:.)f.....}).J..U.v.=..a]c6..<...d..8`...<.....,.....Y.;."...m`#.Nw#p.k.GGAo..q..y.D..F.$...^..8...t...\.=..O.;q..T_.,.....X...8...|{...?.U.*.c...H`\.2 p<.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\umciavi64[1].exe

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1904064
Entropy (8bit):	7.95728490896586
Encrypted:	false
SSDEEP:	49152:QAWal3cWyI5rfPJLPNdm5qzBF07TW+BgSM:13cWjHJjNKqwTWQQ
MD5:	8F727EA574C46E3FD8901335A6548285
SHA1:	185DCF54761BA6FBA7FE4BFFA32F564C9142968D

SHA-256:	D57F75CF079C4EC8C81E51751B3332EF5CE7DC8EBA41B9A5B17DBB4277C20E5C
SHA-512:	B56E01FD3A41408F3655106FBD04F7418D5E13112677B9A36EE4B71B03C23DC7197CF76477DEA3601EFEE8AC46CA6279F02205D1836450C301217B99DD6E2043
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 18%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#c.xg..+g..+g..+yP.+~..+yP.+v..+yP.++..+@..+`..+g..+9..+yP.+e. .+yP.+f..+g..+`..+yP.+f..+Richg..+.....PE..L...EA.c.....2.....@.....>....5D....@.....P....`;.....0>.....p..... .....8...@.....4.....text...1..... ..`.rdata.....@..@.data....U!.....@....rsrc.....`;.....@..@.r eloc...@...0>..B.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Emit64[1].exe

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	10420736
Entropy (8bit):	7.967761917775609
Encrypted:	false
SSDEEP:	196608:Y6khIBSOhjcHmRfm+kXHqxafG8Sc+5jECye/4MqG2naCGl/:Y6khXw8yf9kXEaOG+4Cf4MqG2najI
MD5:	7A5155B804E592D83F8319CBDB27E164
SHA1:	DA63718377B9086EF7F6DB6B8B88E45062F31749
SHA-256:	5EB7B2FD13264F066B10946539EFF6BE750647DE246CF791E57CA4C17B0B9C31
SHA-512:	3DBD6745D7B64EF2260E14DF08C6AA36EE7E34B218DC11C83F5FBCAA934CF1385E79D208E061B9055C389CD5259AE2081B8DEA47FAC38844A2043B9A361D03 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....hr.....!..L.!This program cannot be run in DOS mode....$.....PE..d....E.c.....&.....;....j.....@.....93.. ..`... .....x....p..]... ....9.....`.....}.(.....pv.....87*qGv;7.....`..`^NsFAbb[.M:..... .....@...4.ps1S["....P;.....@..@I^D/X#s1.....p;.....@..@aAyXB94]x.....;.....@..@n9Mms2uS8....;.....7u=]29J1,....;..... .....@...*<5LK<h`h.....;.....@...Ug$Va';z.....;.....@...dA:<*dF(..:...;..... ..`r,Ht]nHV@....pv.....@...m$m2M1,9,....v.....`..ho? %]P5WI.....`.....@..@INMkoK?T]....p.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7705824
Entropy (8bit):	7.9708080300718365
Encrypted:	false
SSDEEP:	196608:ZQoqS56OZEssxxpKIIue41Cf7sgZz6kmAZQ/9RWB0:dMOevKiB1CfQgplmz/9a0
MD5:	2B62E02B3581980EE5A1DDA42FA4F3FE
SHA1:	5C36BFA4A4973E8F694D5C077E7312B1C991AEDF
SHA-256:	8C46C2AF1CB25BFA8FBBF9D683D72D30DDB2E5D0ECC6BBA997B24714CF2B8C91
SHA-512:	255E1B1D51D52872C5E0C54F7807ADC3581D36B3DFB8220C818AC38AC7FCEA91DD42999EE6CCAEF3B9836CD59FCFE19C2669A5B697D627DE4C1D9B8BA563 B3D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....X.....@.....*.u. .....O...X>..@.....~u.....F.....f5g\gWe7..... ..`zDthL)*@.....@...nb"h! m#Y.....$^+<%+dU&.....@...Z-).j99tO.....@..P8"ikKHD[b.C..... ..`k&l<0?<6.....F.....@...n[uZh3ex.lu...F ..nu..... ..`Uh%r6i!H.....xu.....@..P.....@.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\minor[2].bin

Process:	C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe
File Type:	data
Category:	dropped
Size (bytes):	390144
Entropy (8bit):	7.251656172909331
Encrypted:	false
SSDEEP:	6144:TyJP9b+SBjVE9SwQujS2OFhXawQZQbfVYCPmD:TyJP9bFBjVyL5VOFhXCQbfvS
MD5:	BB060F913C31077DB53E3BA747DF6D02
SHA1:	C0184DEDF5B81927218123F4C0E41FABAA090106

SHA-256:	C842C3C50C61E6F44292A6B097F4CB27E1C5E26E87B223C5E017996F25C926CC
SHA-512:	3A2D57D63573869646196FD26FDA98083509248E77745C4E563E8C21771C23C726565280584DF2D3A972DB47349558F7366FFEDE1C42EA44B6998C14D62ADE80
Malicious:	false
Preview:	X@ld.cgvw.:S......)..gv7.........)6Acgvw.........)6Acgvw...M......8A.n.V:..p.|i.F3.........a:KSa...W......xuMSonj|S.........5...&..x... .D1pf...&...d. ...Cf...&.... ...kf...&....v. ....f...&...r. ...uf...&%..... ...)6Acgvw.......E_)6.bcvI.7......)6.cew|.........+6Acgv.........J*6Ac'vw.........(6Acgvr.........,6Aggvw.....k..96Asgvw.........)6Qcgvw........*-6}cgvw.........)6Acgvw.........,6.]gvw.........)6Acgvw.........)6Acgv..........)6Acgvw........)6Acgvw.........)6AcgvY........Z*6Asgvw........)6Acgvw......;hMW5.gvwr........)6A3dvw.........)6.cg6Y........z(6A#cvw.......)6Acgvw......*;hLZ..gvw...e...J)6A.bvw.........)6.cg4w.........)6Acgv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\nppshell[1].exe

Process:	C:\Users\user\Desktop\DQxttu2Qrr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7732440
Entropy (8bit):	7.8779499305543865
Encrypted:	false
SSDEEP:	196608:U+rNR2F7EU+iE09OKsRk3PdM+i+8lHFL9AYS:/RWEU+1OP6+X+oYS
MD5:	2239A58CC93FD94DC2806CE7F6AF0A0B
SHA1:	F09EB7D69BC7440D3D45E14267236A78AC789FCB
SHA-256:	682ABD62B6E3C0E8CA57F079CD96F2D3848752EAF7002BDF57BFB512BD242811
SHA-512:	F77C16626A0E17FF79B95F9FDED6A365F913896C89BAF76D16BCC8706F3AD10A9476C7CBD3F235250B936171C6E958E145C402952506DC0E434A4F911C99FE0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.........XH..6...6...6...5...6...3.a.6...2...6.(.2...6.(.5...6.(.3...6...7...6...7.\.6.f.?...6.f.....6.f.4...6.Rich..6.........PE..L....6.c....................r.......FU...........@..............................~.v...@.................................p......`..`c............u......P......0E..p..........................A..@.............A.h..........................lB@dO\ih.......................... ..`Fh?jG[OJL.........................@..@qNR5:WbSLD.........................@...z?fd8ijJh.=........................ ..`CV?7x>JO......A.....................@...EVjKc_MI.wo...A..xo................ ..`dT<:EHzj.....P........o............@..@@]topACL`c...`...\....o............@..@...

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	45177
Entropy (8bit):	5.072498410577891
Encrypted:	false
SSDEEP:	768:PkWNxV3IpNBQkj25h4iUxuaV7frRJv5FVvCxHBG75ard35n9QOdBQNWzktAHkaN2:PkAxV3CNBQkj25h4iUxuaV7flJnVv6HA
MD5:	79EA83B42F934BED47A1B30D85AB0999
SHA1:	D5AD1B90152F5C698A714FC8044C52571EFCD57B
SHA-256:	9DDA715941C069B34C2052F8902BD6FE9C4956DD2F9E8713F8AD72032BD9662B
SHA-512:	6BDD1F73F199EE5A8BC2EB6FF1B13197E1303B2548932F071EA67A657B5D0056605C5FFC3BAEC02AFDF29A5425BCFA003BA607041A462C2A851B59AF0999567C
Malicious:	false
Preview:	PSMODULECACHE.F..._.>....?...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PKI\PKI.psd1........Export-Certificate........Get-CertificateNotificationTask........Get-PfxData........New-CertificateNotificationTask........Import-PfxCertificate....#...Set-CertificateAutoEnrollmentPolicy........Export-PfxCertificate........Switch-Certificate........New-SelfSignedCertificate....%...Get-CertificateEnrollmentPolicyServer....%...Add-CertificateEnrollmentPolicyServer....(...Remove-CertificateEnrollmentPolicyServer........Import-Certificate........Test-Certificate........Get-Certificate...."...Remove-CertificateNotificationTask....#...Get-CertificateAutoEnrollmentPolicy........_t.....q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1........Set-DAEntryPointTableItem....#...Set-DAClientExperienceConfiguration...."...Enable-DAManualEntryPointSelection........Get-DAEntryPointTableItem........Reset-DAEntryPointTableItem....%...R

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:Nlllulb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943

Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe

Process:	C:\ProgramData\6131289994261301183 2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7732440
Entropy (8bit):	7.8779499305543865
Encrypted:	false
SSDEEP:	196608:U+rNR2F7EU+iE09OKsRk3PdM+i+8lHFL9AYS:/RWEU+1OP6+X+oYS
MD5:	2239A58CC93FD94DC2806CE7F6AF0A0B
SHA1:	F09EB7D69BC7440D3D45E14267236A78AC789FCB
SHA-256:	682ABD62B6E3C0E8CA57F079CD96F2D3848752EAF7002BDF57BFB512BD242811
SHA-512:	F77C16626A0E17FF79B95F9FDED6A365F913896C89BAF76D16BCC8706F3AD10A9476C7CBD3F235250B936171C6E958E145C402952506DC0E434A4F911C99FE0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....XH..6...6...6...5...6...3.a.6...2...6.(.2...6.(.5...6.(.3...6...7...6...7.\.6.f.?...6.f.....6.f.4...6.Rich..6.....PE..L....6.c.....r.....FU.....@.....~.v...@.....p.....`..`c.....u.....P.....0E..p.....A..@.....A.h.....lB@dO\ih..... ..`Fh?jG[OJL.....@..@qNR5:WbSLD.....@...z?fd8ijJh.=..... ..`CV?7x>JO.....A.....@...EVjKc_MI.wo...A..xo..... ..`dT<:EHzj.....P.....o.....@..@@]topACL`c...`...\....o.....@..@..... .....

C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	10420736
Entropy (8bit):	7.967761917775609
Encrypted:	false
SSDEEP:	196608:Y6khIBSOhjcHmRfm+kXHqxafG8Sc+5jECye/4MqG2naCGI/:Y6khXw8yf9kXEaOG+4Cf4MqG2najI
MD5:	7A5155B804E592D83F8319CBDB27E164
SHA1:	DA63718377B9086EF7F6DB6B8B88E45062F31749
SHA-256:	5EB7B2FD13264F066B10946539EFF6BE750647DE246CF791E57CA4C17B0B9C31
SHA-512:	3DBD6745D7B64EF2260E14DF08C6AA36EE7E34B218DC11C83F5FBCAA934CF1385E79D208E061B9055C389CD5259AE2081B8DEA47FAC38844A2043B9A361D036
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....hr.....!..L.!This program cannot be run in DOS mode....$.....PE..d....E.c.....&.....;....j.....@.....93.....`... .....x....p..].... ....9.....`.....}.(.....pv.....87*qGv;7.....`..`^NsFAbb[.M:.....@...4.ps1S["....P;.....@..@I^D/X#s1.....p;.....@..@aAyXB94]x.....;.....@..@n9Mms2uS8.....;.....7u=]29J1,.....;.....@...*<5LK<h`h.....;.....@...Ug$Va';z.....;.....@...dA:<*dF(..:...;..... ..`r,Ht]nHV@....pv.....@...m$m2M1,9,....v.....`..ho?%]P5WI.....`.....@..@INMkoK?T]....p.....@.....

C:\Users\user\AppData\Local\Temp\853321935212

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, components 3
Category:	dropped
Size (bytes):	88895
Entropy (8bit):	7.902972654740771
Encrypted:	false
SSDEEP:	1536:Cu/yFa8aSpJUjE6Ek9wKMp1sOJY1RoBIKSlj536Qz3W+a7WBhiVxp669/O5NI:DmppJQE6r9wx1skvSlIQz3g7WKhhOF
MD5:	2AA81F8E661178C0356A745077A6F304
SHA1:	6B3AEC842EE1F1263E149BEE9967C05109790F80
SHA-256:	1025BEC84A2857436C318823F02844346FDCF00FA198C9D63A27F0F4A3444B66
SHA-512:	22EBB3D2AAEC81AEB3ED1AF5C09A9D36D709BE6AFFDEE978BF808A3D9E82373051822D6CC7B169933C2BD1604ED6C4F4118C7F0606209396E71440828036CE3
Malicious:	false

Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c.....^s.....u,-n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L..... .....H.#.|..).?.H.'.|....).?m.....h.t.....|4.%...d....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fzpuqn5z.g0g.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yjjnzwnv.xjd.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\advapi32.dll

Process:	C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	278528
Entropy (8bit):	6.627837746051642
Encrypted:	false
SSDEEP:	3072:qYGY6mGusO/wtnmpq8ccNmHwJJaPKkZkeXHYOnH60CNAebrMVfEgQ148:qBX5zmg8yfPtZki4Onale3Mxgv
MD5:	ECD0223B882A0FFC6CB684F8202E2FAA
SHA1:	A593370F83C0A9C3FFBD61ED429BCD3A34230D03
SHA-256:	A6A1BCC21608031B8166935904D7ACA16512CAB6296A28D924772BEBAF1DD1DB
SHA-512:	0BCD5DC93AF4A3ACA58D7634F209C7BCD9052D93E68B76A49CA346DE1D11604068B5D201503578B4966F1CAA4484361BF7F87C0F474696D15852260DCCE286A C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....N.c.....!.....2.....`.....@..... .....h.....d.....@.....@.....text..... ..`.data..... .....@....reloc.....@....." .....@..B.....U..SV..|.E..E..E..E...)....)..1.....M.....$..E..E.6.W.E...|...-.....$.....|...-#kC... %.....|...-#h.....-.....|...-.}.....|...-."...F..... .|...-M.....|...-~`.....|...-:Dk.... .....|...-.+&...H#.....|...-B....'.....|...-..4...?$.....|...-..x...,.....|...-.....&.....|...-.....|...-..Z.....|...-..5...'.....|...-$.....r+.....|...-}.....+.....|...-.....

C:\Users\user\AppData\Local\Temp\jekppnay.tmp

Process:	C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe

File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	155136
Entropy (8bit):	7.7612316741526906
Encrypted:	false
SSDEEP:	3072:8QpsuldSMGh+tWWP286pB7YnaEV2d77rRzCLghAaeSdk4cXjU8D5BCG3MSrOUhEa:8QpsuldSMGh+288BYTOVCUhAL4ajlHCc
MD5:	9DE1DECE6C8E92D128133FC779F07AD3
SHA1:	02CC6BD7775D7D024DB6E5AE3DAFE9F8FF001ECB
SHA-256:	3C6AC3153ECB32704D9CD808BFA8872275DD7ED0A49E9709A55FC3511A0AAC4B
SHA-512:	CB1E68792F6BA2994AE30482D6316EE04BFDAC72B8CCCC190BF1F0680D72E59A201732C934D918EA987DD966F0FB8A66100ABFBE27CA4506EDFBF5DF747D45 58
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....hr.....!..L.!This program cannot be run in DOS mode....$.....1a..P...P...P...;...P...;...P...P...P..,)...P..,)...P...P...P..,)...P.. Rich.P.....PE..d.....[c....."....."....H.....8.....@.....`.....PK.....`...%...P..x.....8I..8..... .....0.....text..... ..`.rdata.....0... .....@..@.pdata..x....P.....6.....@..@.rsrc....%...`...&...8.....@..@..... ....

C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1904064
Entropy (8bit):	7.95728490896586
Encrypted:	false
SSDEEP:	49152:QAWal3cWyI5rfPJLPNdm5qzBF07TW+BgSM:13cWjHJjNKqwTWQQ
MD5:	8F727EA574C46E3FD8901335A6548285
SHA1:	185DCF54761BA6FBA7FE4BFFA32F564C9142968D
SHA-256:	D57F75CF079C4EC8C81E51751B3332EF5CE7DC8EBA41B9A5B17DBB4277C20E5C
SHA-512:	B56E01FD3A41408F3655106FBD04F7418D5E13112677B9A36EE4B71B03C23DC7197CF76477DEA3601EFEE8AC46CA6279F02205D1836450C301217B99DD6E2043
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 18%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#c.xg..+g..+g..+yP.+~..+yP.+v..+yP.++..+@..+`..+g..+9..+yP.+e. .+yP.+f..+g..+`..+yP.+f..+Richg..+.....PE..L...EA.c.....2.....@.....>.....5D....@.....P....`;.....0>.....p..... .....8...@.....4.....text...1..... ..`.rdata.....@..@.data....U!.....@....rsrc.....`;.....@..@.r eloc...@...0>..B.....@..B..... .....

C:\Users\user\AppData\Roaming\1000021000\umciavi32.exe

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1678464
Entropy (8bit):	7.9507150099938295
Encrypted:	false
SSDEEP:	49152:20ldRpIqyIKbA+iRYknKnO3YnQI/vKXBs:2+RpalKbdNkKnO3YnQI/vms
MD5:	B66347E9A4018F257A6BF1941B4A5D60
SHA1:	0F4A358AD14E441F74C634054D798E6BE2DA476D
SHA-256:	D74BF0394DE0AD2ADCFD7ECC96711BAC682F3749F8953701EEFC596B8C11DD36
SHA-512:	EAB7414A3D2ED2AAB80EB4452E8B30B6E7481E7CB48BDB986450196EA8695008F7B26D3EE423934A0D6B30650CCD3E50B64CC979723D9DF2DF31052875C046 5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\AppData\Roaming\1000021000\umciavi32.exe, Author: Joe Security
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....NSBGANBRBZHTLGXNSXICJRIHFRNKTLYIZVLK QZWZZIPOYNKNILJIIOVPNXKJVVPH.....Xy..PE..L....^B*.....x.....@.....`.....@.....0...,. .....Xy..(#.....#.....CODE.....w.....x..... ..`DATA..... ...|.....@...BSS.....E.....idata..... .....@....tls.....rdata.....@..P.reloc...#.....$.....@..P.rsrc.....0.....@..P.....P.....@..P..... .....

C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll

Process:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7705824
Entropy (8bit):	7.9708080300718365
Encrypted:	false
SSDEEP:	196608:ZQoqS56OZEssxxpKIIue41Cf7sgZz6kmAZQ/9RWB0:dMOevKiB1CfQgplmz/9a0
MD5:	2B62E02B3581980EE5A1DDA42FA4F3FE
SHA1:	5C36BFA4A4973E8F694D5C077E7312B1C991AEDF
SHA-256:	8C46C2AF1CB25BFA8FBBF9D683D72D30DDB2E5D0ECC6BBA997B24714CF2B8C91
SHA-512:	255E1B1D51D52872C5E0C54F7807ADC3581D36B3DFB8220C818AC38AC7FCEA91DD42999EE6CCAEF3B9836CD59FCFE19C2669A5B697D627DE4C1D9B8BA563B3D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 12%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....X.....@.....*.u. .....O...X>..@.....~u.....F.....f5g\gWe7..... ..`zDthL)*@.....@...nb"h! m#Y.....$^+<%+dU&.....@...Z-),j99tO.....@..P8"ikKHD[b.C..... ..`k&l<0?<6.....F.....@...n[uZh3ex.lu...F ..nu..... ..`Uh%r6i!H.....xu.....@..P.....@.....@..P..... .....

C:\Users\user\Locktime\RtkAudUService64.exe

Process:	C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	10420736
Entropy (8bit):	7.967761917775609
Encrypted:	false
SSDEEP:	196608:Y6khIBSOhjcHmRfm+kXHqxafG8Sc+5jECye/4MqG2naCGI/:Y6khXw8yf9kXEaOG+4Cf4MqG2najI
MD5:	7A5155B804E592D83F8319CBDB27E164
SHA1:	DA63718377B9086EF7F6DB6B8B88E45062F31749
SHA-256:	5EB7B2FD13264F066B10946539EFF6BE750647DE246CF791E57CA4C17B0B9C31
SHA-512:	3DBD6745D7B64EF2260E14DF08C6AA36EE7E34B218DC11C83F5FBCAA934CF1385E79D208E061B9055C389CD5259AE2081B8DEA47FAC38844A2043B9A361D036
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....hr.....!..L.!This program cannot be run in DOS mode....$.....PE..d....E.c.....&.....;....j.....@.....93.. ..`... .....x....p..]... ....9.....`.....}.(.....pv.....87*qGv;7.....`..`^NsFAbb[.M:..... .....@...4.ps1S["....P;.....@..@I^D/X#s1.....p;.....@..@aAyXB94]x....;.....@..@n9Mms2uS8.....;.....7u=]29J1,....;..... .....@...*<5LK<h`h....;.....@...Ug$Va';z.....;.....@...dA:<*dF(..:...;..... ..`r,Ht]nHV@....pv.....@...m$m2M1,9,....v.....`..ho? %]P5WI.....`.....@..@INMkoK?T]....p.....@.....

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2748
Entropy (8bit):	4.269302338623222
Encrypted:	false
SSDEEP:	48:vDZhyoZWM9rU5fFcDL6iCW1RiJ9rn5w0K:vDZEurK9XiCW1RiXn54
MD5:	7B1D6A1E1228728A16B66C3714AA9A23
SHA1:	8B59677A3560777593B1FA7D67465BBD7B3BC548
SHA-256:	3F15965D0159A818849134B3FBB016E858AC50EFDF67BFCD762606AC51831BC5
SHA-512:	573B68C9865416EA2F9CF5C614FCEDBFE69C67BD572BACEC81C1756E711BD90FCFEE93E17B74FB294756ADF67AD18845A56C87F7F870940CBAEB3A579146A3B6
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....0.0.0.0 avast.com..0.0.0.0 www.avast.com..0.0.0.0 totalav.com..0.0.0.0 www.totalav.com..0.0.0.0 scanguard.com..0.0.0.0 www.scanguard.com..

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\cacls.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	15
Entropy (8bit):	3.240223928941852
Encrypted:	false
SSDEEP:	3:o3F:o1
MD5:	509B054634B6DE74F111C3E646BC80FD
SHA1:	99B4C0F39144A92FE42E22473A2A2552FB16BD13
SHA-256:	07C7C151ADD6D955F3C876359C0E2A3A3FB0C519DD1E574413F0B68B345D8C36
SHA-512:	A9C2D23947DBE09D5ECFBF6B3109F3CF8409E43176AE10C18083446EDE006E60E41C3EA2D2765036A967FC81B085D5F271686606AED4154AE45287D412CF6D4
Malicious:	false
Preview:	processed dir:

\Device\Mup\computer\PIPE\samr	
Process:	C:\Users\user\1000018002\avicapn32.exe
File Type:	GLS_BINARY_LSB_FIRST
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.053374040827532
Encrypted:	false
SSDEEP:	3:rmHD/tH//lllLGlA1yqGlgZty:rmH2oty
MD5:	080E701E8B8E2E9C68203C150AC7C6B7
SHA1:	4EF041621388B805758AE1D3B122F9D364705223
SHA-256:	FE129AE2A7C96708754F6F51091E6E512C9FEACA1042A1E9DB914C651FEB344D
SHA-512:	C11D88B8E355B7B922B985802464B693F75BA4C2A62F9137A15842CA82F9B6B3ED13059EDC0DF1C04E7DE43719D892B4C0D22BB67BE0D57EAB368BA1BC057E79
Malicious:	false
Preview:	.....t.....xW4.4.....#Eg.....]..... .+.H`.....xW4.4.....#Eg.....,..l..@E.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.969714456944802
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DQxttu2Qrr.exe
File size:	7387352
MD5:	7434b42e11380272961c92e061072e78
SHA1:	a2dea715e33a860dc09d09b219db18831e6bb1a5
SHA256:	9922432bfa7768bdfb6e8b079c90744c9f3d33a5a258a97abc8519f81a680e40
SHA512:	b426ec3a12c39bfdbf6a52a2971a44e471a76ca270c0aa2ed9b9bb8f1ad5f48f80e7a86659375a05782964762bc3a56f0aa3de87ac509b01c0cad421f8f46a49
SSDEEP:	196608:xhWCcb/OtOBzdC0yo7R5aZPPrf4e0dNL4lkPZFsSM:xhWtb/OtOm0yo3alDfzUNPGZFM
TLSH:	AB76236317255189F4E1CC385637FEE572F3075A8B41BCBED4EAACC128275A4E223A53
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....V.c.....<.....L.....P....@.....`.....<sq...@.....

File Icon

Icon Hash:	c2aaa2abc3cbd200

Static PE Info

General

Entrypoint:	0x8c1e86
Entrypoint Section:	.rrt02
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x638E5699 [Mon Dec 5 20:37:45 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	f27ebcbe4049b07f90dd3733790155ae

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=uncommon company
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/7/2022 5:06:50 PM 12/7/2023 5:26:50 PM
Subject Chain	• CN=uncommon company
Version:	3
Thumbprint MD5:	9938EB0DDDE3DAAE762B8C69C1C53709
Thumbprint SHA-1:	20DF2B39D7CCE671B34083E127FBD5E7C744ABC4
Thumbprint SHA-256:	2567E5A6A91E9CD4EF79CB21D4CAEF2034B5A0FEE7B2EF0B5144A213DDDEAEEA
Serial:	1DFD1A0BD6CE1085439899F76E6C0329

Entrypoint Preview

Instruction
call 00007FB5AD149BF4h
bswap eax
dec eax
rol eax, 1
jmp 00007FB5ACF910E9h
lea eax, dword ptr [eax+689F7F47h]
test eax, edx
bswap eax
lea eax, dword ptr [eax-2DF61256h]
jmp 00007FB5ACF96FCBh
push esi
ret
jmp edi
movsx edi, bx
mov edi, eax
jmp 00007FB5ACF24E97h
jmp ebp
bswap ecx
jmp 00007FB5ACFAFC3Fh
jmp 00007FB5AD0A7DDDh
inc ecx
cmp ebp, esi
xor ebx, ecx
add esi, ecx

Instruction
jmp 00007FB5ACF74494h
not ecx
xor ebx, ecx
cmp dh, 0000000Ch
clc
add esi, ecx
jmp 00007FB5AD589852h
inc al
stc
rol al, 1
cmp ebx, esi
test eax, eax
xor al, 05h
xor bl, al
clc
cmc
mov word ptr [esp+eax], cx
movzx ecx, bp
lea edi, dword ptr [edi-00000004h]
mov ecx, dword ptr [edi]
cmp esp, 027A612Bh
jmp 00007FB5AD0D3C61h
add ebp, 00000004h
test bx, sp
test bp, 2D70h
xor ecx, ebx
jmp 00007FB5AD18D545h
inc edx
test edi, eax
cmp esi, esi
clc
xor ebx, edx
test bp, 0237h
add ebp, edx
jmp 00007FB5AD1387EEh
bswap eax
stc
cmp ebx, edi
clc
xor ebx, eax
test ebp, 50FE79FEh
cmp esi, 1A032DD5h
add esi, eax
jmp 00007FB5ACEEC384h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4d6d88	0x64	.rrt02
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb41000	0x45e6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x70a200	0x16d8	.rrt02
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb40000	0x5f0	.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	0xb3f810	0x40	.rrt02
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x43a000	0x38	.rrt01
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	0x33a16	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x35000	0xe72e	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x44000	0x15164	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rrt00	0x5a000	0x3dfebf	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rrt01	0x43a000	0x4c4	0x600	False	0.040364583333333336	data	0.22812778826287236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rrt02	0x43b000	0x704ab0	0x704c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0xb40000	0x5f0	0x600	False	0.5403645833333334	data	4.361633265576557	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xb41000	0x45e6	0x4600	False	0.094140625	data	2.603551470689515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb411d4	0x313	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0xb414e8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0xb43a90	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0xb44b38	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_GROUP_ICON	0xb44fa0	0x3e	data	English	United States
RT_VERSION	0xb44fe0	0x41c	data		
RT_MANIFEST	0xb453fc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
KERNEL32.dll	LocalAlloc
KERNEL32.dll	GetSystemTimeAsFileTime
USER32.dll	CharUpperBuffW
KERNEL32.dll	LocalAlloc, LocalFree, GetModuleFileNameW, ExitProcess, LoadLibraryA, GetModuleHandleA, GetProcAddress

Possible Origin

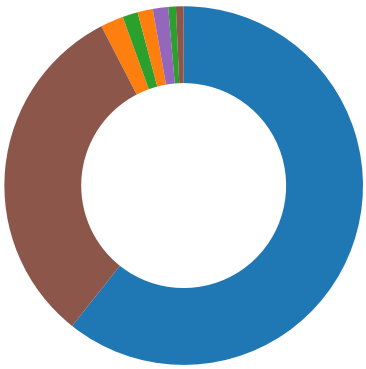
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- DQxttu2Qrr.exe
- 6131289994261301 1832.exe
- cmd.exe
- conhost.exe
- timeout.exe
- gntuud.exe
- schtasks.exe
- conhost.exe
- cmd.exe
- conhost.exe
- cmd.exe
- cacls.exe
- cacls.exe
- cmd.exe
- cacls.exe
- cacls.exe
- rundll32.exe
- gntuud.exe
- Emit64.exe
- avicapn32.exe
- cmd.exe
- cmd.exe
- conhost.exe
- conhost.exe
- powershell.exe
- sc.exe
- conhost.exe
- powercfg.exe
- sc.exe
- powercfg.exe
- sc.exe
- powercfg.exe
- sc.exe
- sc.exe
- powercfg.exe
- reg.exe
- rundll32.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- umciavi64.exe

Click to jump to process

System Behavior

Analysis Process: DQxttu2Qrr.exe PID: 2508, Parent PID: 3452

General

Target ID:	0
Start time:	10:38:07
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\DQxttu2Qrr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DQxttu2Qrr.exe
Imagebase:	0x1090000

File size:	7387352 bytes
MD5 hash:	7434B42E11380272961C92E061072E78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.300367960.00000000010C5000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.298618389.000000000079A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: 6131289994261301183 2.exe PID: **5372**, Parent PID: **2508**

General

Target ID:	4
Start time:	10:38:27
Start date:	09/12/2022
Path:	C:\ProgramData\6131289994261301183 2.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\6131289994261301183 2.exe"
Imagebase:	0x1150000
File size:	7732440 bytes
MD5 hash:	2239A58CC93FD94DC2806CE7F6AF0A0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000004.00000002.327105294.0000000001151000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 35%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\03bd543fce	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	115B6F6	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.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	115B852	CopyFileA

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\03bd543fce\gntuud.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 58 48 fd fd 36 1b fd fd 36 1b fd fd 36 1b fd fd 35 1a fd fd 36 1b fd fd 33 1a 61 fd 36 1b fd fd 32 1a fd fd 36 1b 28 fd 32 1a fd fd 36 1b 28 fd 35 1a fd fd 36 1b 28 fd 33 1a fd fd 36 1b fd fd 37 1a fd fd 36 1b fd fd 37 1b 5c fd 36 1b 66 fd 3f 1a fd fd 36 1b 66 fd fd 1b fd fd 36 1b 66 fd 34 1a fd fd 36 1b 52 69 63 68 fd fd 36 1b 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08	MZ@!L!This program cannot be run in DOS mode.$XH666563a626(26(56(36767\6f?6f6f46Rich6PEL	success or wait	15	115B852	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5596**, Parent PID: **2508**

General

Target ID:	9
Start time:	10:38:30
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "C:\Users\user\Desktop\DQxttu2Qrr.exe" & exit
Imagebase:	0xb0000
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\DQxttu2Qrr.exe	cannot delete	1	D0374	DeleteFileW
C:\Users\user\Desktop\DQxttu2Qrr.exe	cannot delete	1	D0374	DeleteFileW

Analysis Process: conhost.exe PID: **5604**, Parent PID: **5596**

General

Target ID:	10
Start time:	10:38:30
Start date:	09/12/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: timeout.exe PID: **5636**, Parent PID: **5596**

General

Target ID:	11
Start time:	10:38:31
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 6
Imagebase:	0xc50000
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

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: gntuud.exe PID: **5780**, Parent PID: **5372**

General

Target ID:	13
Start time:	10:38:39
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe"
Imagebase:	0x3d0000
File size:	7732440 bytes
MD5 hash:	2239A58CC93FD94DC2806CE7F6AF0A0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 35%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\c33e9ad058e5d3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3E199C	CreateDirectoryA
C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3D8BC2	CreateFileA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA
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	3D9D90	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1000017001\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3DE6C9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3D8BC2	CreateFileA
C:\Users\user\1000018002\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3DE6C9	CreateDirectoryA
C:\Users\user\1000018002\avicapn32.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3D8BC2	CreateFileA
C:\Users\user\1000019012\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3DE6C9	CreateDirectoryA
C:\Users\user\1000019012\syncfiles.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3D8BC2	CreateFileA
C:\Users\user\AppData\Roaming\1000020000\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3DE6C9	CreateDirectoryA
C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3D8BC2	CreateFileA
C:\Users\user\AppData\Roaming\1000021000\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3DE6C9	CreateDirectoryA
C:\Users\user\AppData\Roaming\1000021000\umciavi32.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3D8BC2	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	success or wait	15	3EF6D5	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\Roaming\c33e9ad058e5d3\cred64.dll	0	16384	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 19 5e 42 2a 00 00 00 00 00 00 00 00 fd 00 fd fd 0b 01 02 19 00 fd 01 00 00 58 00 00 00 00 00 00 fd fd fd 00 00 10 00 00 00 fd 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 fd fd 00 00 04 00 00 2a fd 75 00 02 00 01 00 00 00 00 00 00 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 2c fd 00 4f 00 00	MZP@!L!This program must be run under Win32$7PEL^B*X@*u,O	success or wait	471	3D8C27	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	16384	16384	fd fd fd 02 fd fd 40 7a 6c fd fd 00 37 20 3d fd 6d fd 78 fd 00 fd 15 0c 11 fd 6d 69 fd 2c fd fd fd 9d 22 23 7e 7f fd fd 1c 00 64 58 1e fd fd fd 70 09 7d 7f fd 47 ce 00 0e fd 1e 7c fd 6f fd 7e fd fd 78 fd fd fd 27 13 fd fd fd fd 23 76 51 7f fd 39 54 63 fd 32 fd 1b 74 7f fd 4f fd 00 0e fd 26 fd fd 0b 3a 31 77 7f 01 75 fd 00 04 fd 26 76 fd 77 15 fd 74 fd 1f fd fd 74 fd fd 1c 3a fd 77 fd fd fd 8b fd 35 57 47 c9 fd fd 2c 64 17 fd 41 23 43 0c fd 5d 33 fd 2d fd fd 24 33 fd 5c fd fd fd f6 fd 2b fd fd 15 10 3c fd 76 77 fd 36 fd fd 03 fd 11 fd 50 fd 6c fd 2b fd 22 7a 09 4d fd 25 6e 33 fd 44 fd fd fd 75 fd fd 30 fd 49 34 fd fd 29 5f 75 fd fd 5c fd 48 61 33 0e d0 fd fd 4a fd fd 4d 73 fd 34 fd 7c 33 27 fd 49 fd fd 61 5d 5d	@zl7=mxmi,#~dXp}G|~x'#vQ9Tc2tO&:1wu&vwtt:w5WG,dA#C]3-$3\+<vw6Pl+"zM%n3D0I4)_u\Ha3JMs4|3'a]]	success or wait	335	3D8C36	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 68 72 fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0e 00 fd 45 fd 63 00 00 00 00 00 00 00 00 fd 00 2e 02 0b 02 02 26 00 fd 00 00 00 fd 3b 00 00 0e 00 00 6a fd fd 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 15 01 00 04 00 00 39 33 fd 00 02 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@hr!L!This program cannot be run in DOS mode.$PEdEc.&;j@93`	success or wait	637	3D8C27	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Emit64[1].exe	16384	16384	36 fd 2e 7d 72 ab 52 fd 50 28 26 1c fd 33 09 fd 49 4e 38 62 fd fd 25 2c fd fd fd fd 7c fd fd 2d fd fd fd fd 71 fd 3b 0e fd fd fd 73 52 3c fd fd fd fd 0d 57 fd fd 0f 56 fd fd 0b fd 0b fd 03 27 fd fd 14 fd fd fd 31 0e fd 5c fd 90 fd fd 17 fd fd 74 fd fd 2f fd 6f 3d 72 74 fd 1c fd fd 47 fd fd fd fd fd 3a fd fd fd 6b fd fd 72 76 fd fd fd fd fd 7b 0d 29 56 3d fd fd 3d 01 fd fd 6c fd 54 5f fd 40 7d 06 fd fd f5 fd fd fd af fd 7b 50 fd fd fd fd fd fd 1c 3a 0c 26 fd fd 76 fd fd 09 fd 63 fd fd fd 78 fd 67 fd fd 0a fd fd 24 fd 08 3f fd 41 0a fd fd fd 66 fd fd 77 fd fd fd fd 17 4d fd fd fd fd fd fd 0d fd 17 7b fd 79 fd fd 03 fd 22 fd 77 59 51 fd fd 51 fd fd 77 0d 38 fd fd 17 fd fd fd 63 fd fd fd fd fd fd 0e fd fd b7 12	6.}rRP(&3IN8b%,|-q;sR<WV'1\t/o =rtG:krv{)V==lT_@}{P:&vcx$?AfM{y"wYQQ8c	success or wait	423	3D8C36	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\avicapn32[1].exe	0	16384	4d 5a fd 00 03 00 04 00 00 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 03 0b 01 03 00 00 fd 23 00 00 fd 04 00 00 00 00 00 fd 54 fd 00 00 10 00 00 00 60 43 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 01 00 01 00 00 00 06 00 01 00 00 00 00 00 00 fd fd 00 00 04 00 00 fd 14 fd 00 02 00 40 fd 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	MZ@!L!This program cannot be run in DOS mode.$PEL#T`C@@	success or wait	1	3D8C09	InternetReadFile
C:\Users\user\1000018002\avicapn32.exe	0	16384	4d 5a fd 00 03 00 04 00 00 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 02 03 0b 01 03 00 00 fd 23 00 00 fd 04 00 00 00 00 00 fd 54 fd 00 00 10 00 00 00 60 43 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 01 00 01 00 00 00 06 00 01 00 00 00 00 00 00 fd fd 00 00 04 00 00 fd 14 fd 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL#T`C@@	success or wait	775	3D8C27	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\avicapn32[1].exe	16384	16384	00 fd 04 24 fd 40 18 00 00 00 00 fd 40 1c 00 00 00 00 fd 4c 24 18 fd fd 0f fd 8b 5c 24 1c fd c7 fd 0f fd c7 fd 09 55 fd fd fd 74 0e fd 40 18 fd fd fd fd 40 1c fd fd fd fd fd 15 fd 2c fd 00 fd fd 75 16 fd 54 24 48 fd 50 0c fd 40 2c 00 00 00 00 fd 6c 24 28 fd 28 fd 2d fd 78 0c fd 8b 44 24 48 fd fd 05 00 fd 7a 2c fd fd 31 fd fd fd 05 00 fd cb 44 24 28 fd fd 05 00 fd fd fd fd 6c 24 28 fd 40 24 00 fd 78 34 fd 35 fd 2c fd 00 fd fd 75 09 fd 74 24 44 fd 70 34 fd 11 fd 8b 44 24 44 fd 70 fd 05 00 fd fd fd 74 24 44 fd 44 24 20 fd 45 00 fd fd fd 00 00 00 fd 0d fd 2c fd 00 fd 55 44 fd fd 75 0f fd fd fd 00 00 00 fd 45 44 00 00 00 00 fd 18 fd fd fd fd fd 38 fd 05 00 fd fd 31 fd fd 2f fd 05 00 fd 44 24 20 fd c9 7c 24 34 fd fd 0d fd	$@@L$\$t@@,uT$HP@,l$((-xD$Hz,1 D$(l$(@$x45,ut$Dp4D$DptDD E,UDuED81/D$ |$4	success or wait	760	3D8C36	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\syncfiles[1].dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 38 fd 6f 62 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 05 0c 00 22 00 00 00 40 00 00 00 00 00 00 3d 58 54 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 fd fd 00 00 04 00 00 fd 46 74 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 2f fd 00 45 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL8ob!"@=XT@Ft/E	success or wait	1	3D8C09	InternetReadFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\1000019012\syncfiles.dll</td><td>0</td><td>16384</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 38 fd 6f 62 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 05 0c 00 22 00 00 00 40 00 00 00 00 00 00 3d 58 54 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 fd fd 00 00 04 00 00 fd 46 74 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 fd 2f fd 00 45 00 00</td><td>MZ@!L!This program cannot be run in DOS mode.$PEL8ob!"@=XT@Ft/E</td><td>success or wait</td><td>462</td><td>3D8C27</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\syncfiles[1].dll</td><td>16384</td><td>16384</td><td>fd fd 5c 2f 48 fd fd 30 fd 6e 53 fd 21 fd fd 36 fd fd fd 2c fd 10 fd 29 fd fd cf 52 6b fd 01 fd 24 5c 23 fd fd cf fd 3d 31 fd fd fd fd fd fd 60 fd 7a fd 6f 72 51 57 fd 42 6a 43 fd 24 fd fd 75 fd fd 22 fd fd 15 fd 22 5b 79 2c 14 6d fd fd fd fd 57 42 fd 11 4d 5c fd fd 44 5d fd fd 6f fd 72 03 fd fd 10 6d 3a fd 77 4e 3d 47 fd 5e fd 41 3d 0f fd fd 27 7d fd 22 fd fd fd fd 22 0f fd fd 3f 6d 73 66 47 b2 fd fd 37 3a 4d fd 26 07 6e 2d 6c 79 fd 06 27 2e 04 11 72 fd fd fd fd fd 7f fd fd 51 fd 72 fd 7f 79 fd 23 fd 7f 70 fd 58 56 20 33 09 fd fd 2d 7a fd fd fd 19 77 fd 46 20 fd 16 fd fd 53 fd 50 50 1a 5a fd fd 60 fd 76 33 fd 11 66 4f fd 09 fd 32 14 70 fd 36 7c 34 65 02 23 fd fd fd 4a 65 fd fd 15 fd 45 1a fd fd fd 3a fd 53 32 fd</td><td>\/HnS!6,)Rk$\#=1`zorQWjC$u""[y,mWBM\D]orm:wN=G^A='}""?msfG7:M&n-ly'.Qry#pXV 3-zwFSPPZ`v3fO2p6|4eJeE:S2</td><td>success or wait</td><td>398</td><td>3D8C36</td><td>InternetReadFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\umciavi64[1].exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 63 fd 78 67 02 fd 2b 67 02 fd 2b 67 02 fd 2b 79 50 02 2b 7e 02 fd 2b 79 50 13 2b 76 02 fd 2b 79 50 05 2b 2b 02 fd 2b 40 fd fd 2b 60 02 fd 2b 67 02 fd 2b 39 02 fd 2b 79 50 0c 2b 65 02 fd 2b 79 50 12 2b 66 02 fd 2b 67 02 11 2b 60 02 fd 2b 79 50 17 2b 66 02 fd 2b 52 69 63 68 67 02 fd 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 45 41 fd 63 00 00 00	MZ@!L!This program cannot be run in DOS mode.$#cxg+g+g+yP+~+yP+v+yP+++@+`+g+9+yP+e+yP+f+g+`+yP+f+Richg+PELEAc	success or wait	1	3D8C09	InternetReadFile
C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 63 fd 78 67 02 fd 2b 67 02 fd 2b 67 02 fd 2b 79 50 02 2b 7e 02 fd 2b 79 50 13 2b 76 02 fd 2b 79 50 05 2b 2b 02 fd 2b 40 fd fd 2b 60 02 fd 2b 67 02 fd 2b 39 02 fd 2b 79 50 0c 2b 65 02 fd 2b 79 50 12 2b 66 02 fd 2b 67 02 11 2b 60 02 fd 2b 79 50 17 2b 66 02 fd 2b 52 69 63 68 67 02 fd 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 45 41 fd 63 00 00 00	MZ@!L!This program cannot be run in DOS mode.$#cxg+g+g+yP+~+yP+v+yP+++@+`+g+9+yP+e+yP+f+g+`+yP+f+Richg+PELEAc	success or wait	117	3D8C27	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\umciavi64[1].exe	16384	16384	0d 00 0d 5a 00 fd 4d fd 33 05 fd 0c 5a 00 33 0d fd 0c 5a 00 0b fd 75 07 fd 01 00 00 00 fd 02 33 fd fd 4d fd 66 0f fd fd 66 fd fd 66 0f fd 0a 45 fd 66 0f fd fd 0f fd 05 fd 0c 5a 00 66 fd fd 66 03 fd 66 fd 15 20 0d 5a 00 fd 55 fd 23 fd 29 55 fd fd fd 0c 5a 00 fd 0d fd 0c 5a 00 fd 15 40 54 7b 00 05 1b fd fd fd fd 45 fd fd fd fd fd 4d 09 55 fd fd 45 fd 00 00 00 00 33 fd 66 fd fd fd fd fd fd 77 fd fd fd fd fd fd 45 fd fd 55 fd fd 45 fd 0b 45 fd 75 5e 0f fd 4d fd fd fd 8a 26 26 fd 4d fd 66 fd 55 fd 0f fd fd 68 22 3a 04 00 fd 68 fd 34 52 50 61 00 00 01 05 fd 0c 5a 00 fd fd 0c 5a 00 0f fd 4d fd 11 15 fd 0c 5a 00 fd fd 02 6d 00 0f fd 05 fd 0c 5a 00 fd fd 15 fd 0c 5a 00 fd 15 fd 0c 5a 00 03 a3 fd 0c 5a 00 fd 4d fd 0f fd 05 fd 0c 5a 00 3b	ZM3Z3Zu3MfffEfZfff ZU#)UZZ@T{E MUE3fwEUEEu^M&&Mf Uh":hRPZZMZmZ ZZZMZ;	success or wait	112	3D8C36	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\umciavi32[1].exe	0	16384	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4e 53 42 47 41 4e 42 52 42 5a 48 54 4c 47 58 4e 53 58 49 43 4a 52 49 48 46 52 4e 4b 54 4c 59 49 5a 56 4c 4b 51 5a 57 5a 5a 49 50 4f 59 4e 4b 4e 49 4c 4a 49 49 4f 56 50 4e 58 4b 4a 56 56 50 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 79 19	MZP@!L!This program must be run under Win32$7NSBGANBRBZ HTLGX NSXICJRIHFRNKTLYIZV LKQZWZZIPOY NKNILJIIOVPNXKJVVPH Xy	success or wait	1	3D8C09	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1000021000\umciavi32.exe	0	16384	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4e 53 42 47 41 4e 42 52 42 5a 48 54 4c 47 58 4e 53 58 49 43 4a 52 49 48 46 52 4e 4b 54 4c 59 49 5a 56 4c 4b 51 5a 57 5a 5a 49 50 4f 59 4e 4b 4e 49 4c 4a 49 49 4f 56 50 4e 58 4b 4a 56 56 50 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 79 19	MZP@!L!This program must be run under Win32$7NSBGANBRBZHTLGXNSXICJRIHFRNKTLYIZVLKQZWZZIPOYNKNILJIIOVPNXKJVVPHXy	success or wait	103	3D8C27	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\umciavi32[1].exe	16384	16384	31 fd fd 41 01 fd 7c 08 0a fd 6f fd 31 fd fd 4f fd 51 fd 4f 04 29 fd 7e 0b fd fd 01 fd 01 fd fd fd fd fd 47 04 fd 17 fd 12 fd 0a fd fd 0a 74 31 fd fd 0b 74 3d fd fd 0c 74 49 fd fd 0d 74 55 fd fd 0e 74 70 fd fd 0f 0f fd fd 00 00 00 fd fd 11 0f fd fd 00 00 00 fd 02 5d 5f 5e 5b fd fd fd fd fd 14 30 01 fd fd fd fd fd 04 00 00 00 fd 7d fd 14 30 01 fd fd fd fd fd 04 00 00 00 fd 6c fd 14 30 01 fd fd 51 fd fd fd 10 00 00 00 fd 5b 31 4a 4a 01 fd 74 11 02 fd 74 11 06 fd 4c 11 0a fd 09 fd 14 30 01 fd fd 61 00 00 00 58 fd 3b 31 4a 4a 01 fd 4c 11 02 51 fd 4d 14 30 01 fd fd 2c fd fd fd 58 fd 22 fd 14 30 01 fd fd 3f 0d 00 00 fd 04 00 00 00 fd 11 fd 4b 14 30 01 fd fd 64 07 00 00 fd 04 00 00 00 03 47 04 fd fd 08 4d 0f fd 14 fd fd fd 59	1A|o1OQO)~Gt1t=tItUtp]_^[0}0l0Q[1JttL0aX;1JLQ0,X"0?0dGMY	success or wait	97	3D8C36	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	unknown	4	success or wait	97492	3D9757	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	syncfiles.dll	expand unicode	rundll32 C:\Users\user\1000019012\syncfiles.dll, rundll	success or wait	1	3D2F97	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	umciavi64.exe	expand unicode	C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe	success or wait	1	3D2F97	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	umciavi32.exe	expand unicode	C:\Users\user\AppData\Roaming\1000021000\umciavi32.exe	success or wait	1	3D2F97	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Startup	expand unicode	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	C:\Users\user\AppData\Local\Temp\03bd543fce\	success or wait	1	3D2F97	RegSetValueExA

Analysis Process: schtasks.exe PID: **5908**, Parent PID: **5780**

General

Target ID:	14
Start time:	10:38:51
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN gntuud.exe /TR "C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe" /F
Imagebase:	0xb30000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5920**, Parent PID: **5908**

General

Target ID:	15
Start time:	10:38:51
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: cmd.exe PID: **5928**, Parent PID: **5780**

General

Target ID:	16

Start time:	10:38:51
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k echo Y|CACLS "gntuud.exe" /P "user:N"&&CACLS "gntuud.exe" /P "user:R" /E&&echo Y|CACLS "..\03bd543fce" /P " user:N"&&CACLS "..\03bd543fce" /P "user:R" /E&&Exit
Imagebase:	0xb0000
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

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5964**, Parent PID: **5928**

General

Target ID:	17
Start time:	10:38:51
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: cmd.exe PID: **5996**, Parent PID: **5928**

General

Target ID:	18
Start time:	10:38:51
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0xb0000
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

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **6004**, Parent PID: **5928**

General

Target ID:	19
Start time:	10:38:51
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "gntuud.exe" /P "user:N"
Imagebase:	0xc20000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
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 Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	19	C249CC	fprintf
\Device\ConDrv	20	1	72	r	success or wait	16	C249CC	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **6024**, Parent PID: **5928**

General

Target ID:	20
Start time:	10:38:52
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "gntuud.exe" /P "user:R" /E
Imagebase:	0xc20000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
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 Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	16	C249CC	fprintf

Analysis Process: cmd.exe PID: **6064**, Parent PID: **5928**

General

Target ID:	21
Start time:	10:38:52
Start date:	09/12/2022

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cacls.exe PID: **6076**, Parent PID: **5928**

General

Target ID:	22
Start time:	10:38:52
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\03bd543fce" /P "user:N"
Imagebase:	0xc20000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
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 Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	19	C249CC	fprintf
\Device\ConDrv	20	1	72	r	success or wait	15	C249CC	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **6096**, Parent PID: **5928**

General

Target ID:	23
Start time:	10:38:53
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\03bd543fce" /P "user:R" /E
Imagebase:	0xc20000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
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 Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	15	C249CC	fprintf

Analysis Process: rundll32.exe PID: **6128**, Parent PID: **5780**

General	
Target ID:	24
Start time:	10:38:56
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\c33e9ad058e5d3\cred64.dll, Main
Imagebase:	0x1250000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Analysis Process: gntuud.exe PID: **4948**, Parent PID: **1080**

General	
Target ID:	25
Start time:	10:39:02
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\03bd543fce\gntuud.exe
Imagebase:	0x3d0000
File size:	7732440 bytes
MD5 hash:	2239A58CC93FD94DC2806CE7F6AF0A0B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000019.00000002.762181339.00000000003D1000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security

Analysis Process: Emit64.exe PID: **3920**, Parent PID: **5780**

General	
Target ID:	26
Start time:	10:39:06
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\1000017001\Emit64.exe"
Imagebase:	0x7ff675890000
File size:	10420736 bytes
MD5 hash:	7A5155B804E592D83F8319CBDB27E164
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs

Analysis Process: avicapn32.exe PID: **1112**, Parent PID: **5780**

General	
Target ID:	27
Start time:	10:39:15
Start date:	09/12/2022
Path:	C:\Users\user\1000018002\avicapn32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1000018002\avicapn32.exe"
Imagebase:	0xbc0000
File size:	12684504 bytes
MD5 hash:	0F6EF96C5E687631EF27F1DCD1AFE7B4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_LaplasClipper, Description: Yara detected Laplas Clipper, Source: 0000001B.00000002.821990980.0000000000E00000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_LaplasClipper, Description: Yara detected Laplas Clipper, Source: 0000001B.00000000.407007293.0000000000E00000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_LaplasClipper, Description: Yara detected Laplas Clipper, Source: C:\Users\user\1000018002\avicapn32.exe, Author: Joe Security
Antivirus matches:	• Detection: 15%, ReversingLabs

Analysis Process: cmd.exe PID: **1500**, Parent PID: **3452**

General	
Target ID:	28
Start time:	10:39:15
Start date:	09/12/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe /c sc stop UsoSvc & sc stop WaaSMedicSvc & sc stop wuauserv & sc stop bits & sc stop dosvc & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\UsoSvc" /f & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\WaaSMedicSvc" /f & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\wuauserv" /f & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\bits" /f & reg delete "HKLM\SYSTEM\CurrentControlSet\Services\dosvc" /f
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2436**, Parent PID: **3452**

General	
Target ID:	29
Start time:	10:39:15
Start date:	09/12/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe /c powercfg /x -hibernate-timeout-ac 0 & powercfg /x -hibernate-timeout-dc 0 & powercfg /x -standby-timeout-ac 0 & powercfg /x -standby-timeout-dc 0
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3076**, Parent PID: **1500**

General	
Target ID:	30
Start time:	10:39:15
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5192**, Parent PID: **2436**

General	
Target ID:	31
Start time:	10:39:16
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **3044**, Parent PID: **3920**

General	
Target ID:	32
Start time:	10:39:16
Start date:	09/12/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe <#qgoyddbo#> IF((New-Object Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) { IF([System.Environment]::OSVersion.Version -lt [System.Version]"6.2") { schtasks /create /f /sc onlogon /rl highest /tn 'RtkAudUService64.exe' /tr '"C:\Users\user\Locktime\RtkAudUService64.exe"' } Else { Register-ScheduledTask -Action (New-ScheduledTaskAction -Execute 'C:\Users\user\Locktime\RtkAudUService64.exe') -Trigger (New-ScheduledTaskTrigger -AtLogOn) -Settings (New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -DisallowHardTerminate -DontStopIfGoingOnBatteries -DontStopOnIdleEnd -ExecutionTimeLimit (New-TimeSpan -Days 1000)) -TaskName 'RtkAudUService64.exe' -RunLevel 'Highest' -Force; } } Else { reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "RtkAudUService64.exe" /t REG_SZ /f /d 'C:\Users\user\Locktime\RtkAudUService64.exe' }
Imagebase:	0x7ff60b350000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: sc.exe PID: **5040**, Parent PID: **1500**

General	
Target ID:	33

Start time:	10:39:16
Start date:	09/12/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc stop UsoSvc
Imagebase:	0x7ff653d10000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5248**, Parent PID: **3044**

General

Target ID:	34
Start time:	10:39:16
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powercfg.exe PID: **1340**, Parent PID: **2436**

General

Target ID:	35
Start time:	10:39:16
Start date:	09/12/2022
Path:	C:\Windows\System32\powercfg.exe
Wow64 process (32bit):	false
Commandline:	powercfg /x -hibernate-timeout-ac 0
Imagebase:	0x7ff6385a0000
File size:	94720 bytes
MD5 hash:	7C749DC22FCB1ED42A87AFA986B720F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **3400**, Parent PID: **1500**

General

Target ID:	36
Start time:	10:39:16
Start date:	09/12/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc stop WaaSMedicSvc
Imagebase:	0x7ff653d10000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powercfg.exe PID: **3508**, Parent PID: **2436**

General

Target ID:	37
Start time:	10:39:17
Start date:	09/12/2022
Path:	C:\Windows\System32\powercfg.exe
Wow64 process (32bit):	false
Commandline:	powercfg /x -hibernate-timeout-dc 0
Imagebase:	0x7ff6385a0000
File size:	94720 bytes
MD5 hash:	7C749DC22FCB1ED42A87AFA986B720F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **4616**, Parent PID: **1500**

General

Target ID:	38
Start time:	10:39:18
Start date:	09/12/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc stop wuauserv
Imagebase:	0x7ff653d10000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powercfg.exe PID: **5604**, Parent PID: **2436**

General

Target ID:	39
Start time:	10:39:21
Start date:	09/12/2022
Path:	C:\Windows\System32\powercfg.exe
Wow64 process (32bit):	false
Commandline:	powercfg /x -standby-timeout-ac 0
Imagebase:	0x7ff6385a0000
File size:	94720 bytes
MD5 hash:	7C749DC22FCB1ED42A87AFA986B720F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **5488**, Parent PID: **1500**

General

Target ID:	40
Start time:	10:39:21
Start date:	09/12/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc stop bits
Imagebase:	0x7ff653d10000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **5224**, Parent PID: **1500**

General

Target ID:	41
Start time:	10:39:21
Start date:	09/12/2022
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	sc stop dosvc
Imagebase:	0x7ff653d10000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powercfg.exe PID: **5836**, Parent PID: **2436**

General

Target ID:	42
Start time:	10:39:22
Start date:	09/12/2022
Path:	C:\Windows\System32\powercfg.exe
Wow64 process (32bit):	false
Commandline:	powercfg /x -standby-timeout-dc 0
Imagebase:	0x7ff6385a0000
File size:	94720 bytes
MD5 hash:	7C749DC22FCB1ED42A87AFA986B720F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **5848**, Parent PID: **1500**

General

Target ID:	43
Start time:	10:39:22
Start date:	09/12/2022
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg delete "HKLM\SYSTEM\CurrentControlSet\Services\UsoSvc" /f
Imagebase:	0x7ff7185b0000
File size:	72704 bytes

MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **2820**, Parent PID: **5780**

General	
Target ID:	44
Start time:	10:39:23
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\rundll32.exe" C:\Users\user\1000019012\syncfiles.dll, rundll
Imagebase:	0x1250000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 0000002C.00000002.809371970.0000000010005000.00000004.00000001.01000000.0000000E.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security

Analysis Process: reg.exe PID: **5772**, Parent PID: **1500**

General	
Target ID:	45
Start time:	10:39:23
Start date:	09/12/2022
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg delete "HKLM\SYSTEM\CurrentControlSet\Services\WaaSMedicSvc" /f
Imagebase:	0x7ff7185b0000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **4864**, Parent PID: **1500**

General	
Target ID:	46
Start time:	10:39:25
Start date:	09/12/2022
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg delete "HKLM\SYSTEM\CurrentControlSet\Services\wuauserv" /f
Imagebase:	0x7ff7185b0000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **1948**, Parent PID: **1500**

General	
Target ID:	47
Start time:	10:39:25
Start date:	09/12/2022
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg delete "HKLM\SYSTEM\CurrentControlSet\Services\bits" /f
Imagebase:	0x7ff7185b0000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **5344**, Parent PID: **1500**

General	
Target ID:	48
Start time:	10:39:25
Start date:	09/12/2022
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg delete "HKLM\SYSTEM\CurrentControlSet\Services\dosvc" /f
Imagebase:	0x7ff7185b0000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: umciavi64.exe PID: **68**, Parent PID: **5780**

General	
Target ID:	49
Start time:	10:39:28
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\1000020000\umciavi64.exe"
Imagebase:	0xbc0000
File size:	1904064 bytes
MD5 hash:	8F727EA574C46E3FD8901335A6548285
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000031.00000002.656321722.000000000F230000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000031.00000002.656321722.000000000F230000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000031.00000003.546951720.000000000F0D2000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000031.00000003.546951720.000000000F0D2000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000031.00000003.619550432.000000000F2F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000031.00000003.539665627.000000000F0D0000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000031.00000003.539665627.000000000F0D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000031.00000003.539665627.000000000F0D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000031.00000003.539665627.000000000F0D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_Arechclient2, Description: Detects Arechclient2 RAT, Source: 00000031.00000003.539665627.000000000F0D0000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 18%, ReversingLabs

Disassembly

No disassembly