ID: 780207
Sample Name: 8082-svc-x86.exe
Cookbook: default.jbs
Time: 16:05:54
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 8082-svc-x86.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: CobaltStrike 4
Yara Signatures 5
Initial Sample 5
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
System Summary 7
Hooking and other Techniques for Hiding and Protection 7
HIPS / PFW / Operating System Protection Evasion 7
Lowering of HIPS / PFW / Operating System Security Settings 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 13
Public IPs 13
General Information 14
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log 15
C:\servicereg.log 15
C:\servicestart.log 15
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 17
Data Directories 18
Sections 18
Imports 20
Network Behavior 21
TCP Packets 21
HTTP Request Dependency Graph 22
Statistics 23
Behavior 23
System Behavior 23
Analysis Process: cmd.exePID: 6060, Parent PID: 1848 23
General 23

File Activities 23
Analysis Process: conhost.exePID: 6068, Parent PID: 6060 23
General 23
Analysis Process: sc.exePID: 6100, Parent PID: 6060 24
General 24
File Activities 24
File Written 24
Analysis Process: cmd.exePID: 3140, Parent PID: 1848 24
General 24
File Activities 24
File Created 24
Analysis Process: conhost.exePID: 2752, Parent PID: 3140 25
General 25
Analysis Process: sc.exePID: 988, Parent PID: 3140 25
General 25
File Activities 25
File Written 25
Analysis Process: 8082-svc-x86.exePID: 1284, Parent PID: 576 26
General 26
File Activities 27
File Read 27
Analysis Process: rundll32.exePID: 3128, Parent PID: 1284 27
General 27
File Activities 27
File Created 27
Analysis Process: svchost.exePID: 2392, Parent PID: 576 29
General 29
Analysis Process: svchost.exePID: 5416, Parent PID: 576 29
General 29
File Activities 29
Analysis Process: svchost.exePID: 4532, Parent PID: 576 29
General 29
Registry Activities 29
Analysis Process: svchost.exePID: 5644, Parent PID: 576 30
General 30
Analysis Process: SgrmBroker.exePID: 4380, Parent PID: 576 30
General 30
Analysis Process: svchost.exePID: 4792, Parent PID: 576 30
General 30
File Activities 30
Registry Activities 31
Analysis Process: svchost.exePID: 5932, Parent PID: 576 31
General 31
Registry Activities 31
Analysis Process: MpCmdRun.exePID: 5448, Parent PID: 5932 31
General 31
File Activities 31
File Written 32
Analysis Process: conhost.exePID: 5512, Parent PID: 5448 33
General 33
Disassembly 33

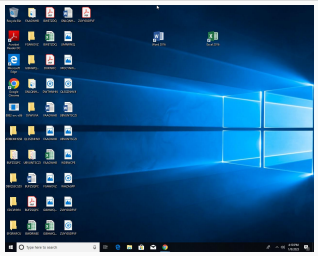
Windows Analysis Report

8082-svc-x86.exe

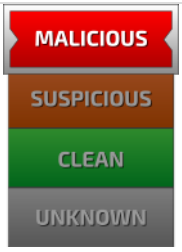
Overview

General Information

Sample Name:	8082-svc-x86.exe
Analysis ID:	780207
MD5:	8fc088eec229a6…
SHA1:	0043b6ba9f8edfd.
SHA256:	deeb89a16aa2b7.
Tags:	45139105143 exe opendir
Infos:	



Detection



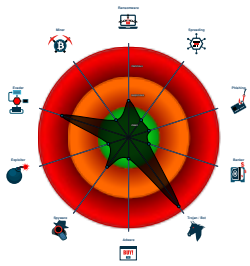
CobaltStrike

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Yara detected CobaltStrike
- Uses known network protocols on n…
- Changes security center settings (n…
- Machine Learning detection for sam…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Found decision node followed by no…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6060 cmdline: cmd /c sc create CfsHz binpath= "C:\Users\user\Desktop\8082-svc-x86.exe" >> C:\servicereg.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 6100 cmdline: sc create CfsHz binpath= "C:\Users\user\Desktop\8082-svc-x86.exe" MD5: 24A3E2603E63BCB9695A2935D3B24695)
- cmd.exe (PID: 3140 cmdline: cmd /c sc start CfsHz >> C:\servicestart.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 2752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 988 cmdline: sc start CfsHz MD5: 24A3E2603E63BCB9695A2935D3B24695)
- 8082-svc-x86.exe (PID: 1284 cmdline: C:\Users\user\Desktop\8082-svc-x86.exe MD5: 8FC088EEC229A693F2D754C67A2E506A)
  - rundll32.exe (PID: 3128 cmdline: C:\Windows\System32\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 2392 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5416 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4532 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5644 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4380 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 4792 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5932 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5448 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: CobaltStrike

```
{
  "BeaconType": [
    "HTTP"
  ],
  "Port": 8082,
  "SleepTime": 38500,
  "MaxGetSize": 1399607,
  "Jitter": 27,
  "C2Server": "20.104.209.69,/broadcast",
  "HttpPostUri": "/1/events/com.amazon.csm.csa.prod",
  "Malleable_C2_Instructions": [
    "Remove 1308 bytes from the end",
    "Remove 1 bytes from the end",
    "Remove 194 bytes from the beginning",
    "Base64 decode"
  ],
  "SpawnTo": "16nKFaB/gr/TtjAg2jiqFg==",
  "HttpGet_Verb": "GET",
  "HttpPost_Verb": "POST",
  "HttpPostChunk": 0,
  "Spawnto_x86": "%windir%\\syswow64\\gpupdate.exe",
  "Spawnto_x64": "%windir%\\sysnative\\gpupdate.exe",
  "CryptoScheme": 0,
  "Proxy_Behavior": "Use IE settings",
  "Watermark": 1670873463,
  "bStageCleanup": "True",
  "bCFGCaution": "True",
  "KillDate": 0,
  "bProcInject_StartRWX": "True",
  "bProcInject_UseRWX": "False",
  "bProcInject_MinAllocSize": 16700,
  "ProcInject_PrependAppend_x86": [
    "kJCQ",
    "Empty"
  ],
  "ProcInject_PrependAppend_x64": [
    "kJCQ",
    "Empty"
  ],
  "ProcInject_Execute": [
    "ntdll.dll:RtlUserThreadStart",
    "SetThreadContext",
    "NtQueueApcThread-s",
    "kernel32.dll:LoadLibraryA",
    "CreateRemoteThread",
    "RtlCreateUserThread"
  ],
  "ProcInject_AllocationMethod": "NtMapViewOfSection",
  "bUsesCookies": "False",
  "HostHeader": ""
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
8082-svc-x86.exe	CobaltStrike_Resources_Artifact32_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact32{.dll,.exe,big.exe,big.dll,bigsvc.exe} signature for versions 3.14 to 4.x and resources/artifact32svc.exe for 3.14 to 4.x and resources/artifact32uac.dll for v3.14 and v4.0	gssincla@google.com	• 0xe07:$pushFmtStr: C7 44 24 28 5C 00 00 00 C7 44 24 24 65 00 00 00 C7 44 24 20 70 00 00 00 C7 44 24 1C 69 00 00 00 C7 44 24 18 70 00 00 00 F7 F1 C7 44 24 14 5C 00 00 00 C7 44 24 10 2E 00 00 00 C7 44 24 0C 5C 00 ... • 0x44a68:$fmtStr: %c%c%c%c%c%c%c%cMSSE-%d-server
8082-svc-x86.exe	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0xbc2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30
8082-svc-x86.exe	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.780101096.00000000010C6000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_CobaltStrike_3	Yara detected CobaltStrike	Joe Security	
00000007.00000002.780610935.0000000003DA0000.00000004.00000800.00020000.00000000.sdmp	SUSP_PS1_FromBase64String_Content_Indicator	Detects suspicious base64 encoded PowerShell expressions	Florian Roth	• 0x70:$: ::FromBase64String("H4s • 0x70:$: ::FromBase64String("H4sIA
00000007.00000002.780610935.0000000003DA0000.00000004.00000800.00020000.00000000.sdmp	CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x	Cobalt Strike\'s resources/cmmand.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x	gssincla@google.com	• 0x48:$ps1: $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(• 0x28f51:$ps2:));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
00000007.00000002.779835594.00000000010A0000.00000020.00001000.00020000.00000000.sdmp	CobaltStrike_Sleeve_Beacon_Dll_v4_3_v4_4_v4_5_and_v4_6	Cobalt Strike\'s sleeve/beacon.dll Versions 4.3 and 4.4	gssincla@google.com	• 0x72da:$version_sig: 48 57 8B F2 83 F8 65 0F 87 47 03 00 00 FF 24 • 0x96c3:$decoder: 80 B0 20 10 0D 01 2E 40 3D 00 10 00 00 7C F1
00000006.00000000.252641646.0000000000401000.00000020.00000001.01000000.00000003.sdmp	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0x7c2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.8082-svc-x86.exe.400000.0.unpack	CobaltStrike_Resources_Artifact32_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact32{.dll,.exe,big.exe,big.dll,bigsvc.exe} signature for versions 3.14 to 4.x and resources/artifact32svc.exe for 3.14 to 4.x and resources/artifact32uac.dll for v3.14 and v4.0	gssincla@google.com	• 0xe07:$pushFmtStr: C7 44 24 28 5C 00 00 00 C7 44 24 24 65 00 00 00 C7 44 24 20 70 00 00 00 C7 44 24 1C 69 00 00 00 C7 44 24 18 70 00 00 00 F7 F1 C7 44 24 14 5C 00 00 00 C7 44 24 10 2E 00 00 00 C7 44 24 0C 5C 00 ... • 0x44a68:$fmtStr: %c%c%c%c%c%c%c%cMSSE-%d-server
6.2.8082-svc-x86.exe.400000.0.unpack	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0xbc2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30
6.2.8082-svc-x86.exe.400000.0.unpack	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	
6.0.8082-svc-x86.exe.400000.0.unpack	CobaltStrike_Resources_Artifact32_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact32{.dll,.exe,big.exe,big.dll,bigsvc.exe} signature for versions 3.14 to 4.x and resources/artifact32svc.exe for 3.14 to 4.x and resources/artifact32uac.dll for v3.14 and v4.0	gssincla@google.com	• 0xe07:$pushFmtStr: C7 44 24 28 5C 00 00 00 C7 44 24 24 65 00 00 00 C7 44 24 20 70 00 00 00 C7 44 24 1C 69 00 00 00 C7 44 24 18 70 00 00 00 F7 F1 C7 44 24 14 5C 00 00 00 C7 44 24 10 2E 00 00 00 C7 44 24 0C 5C 00 ... • 0x44a68:$fmtStr: %c%c%c%c%c%c%c%cMSSE-%d-server
6.0.8082-svc-x86.exe.400000.0.unpack	CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x	Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x)	gssincla@google.com	• 0xbc2:$decoderFunc: 89 C8 BF 04 00 00 00 99 F7 FF 8B 7D E0 8A 04 17 30
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

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

Uses known network protocols on non-standard ports

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

HIPS / PFW / Operating System Protection Evasion

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

Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

Remote Access Functionality

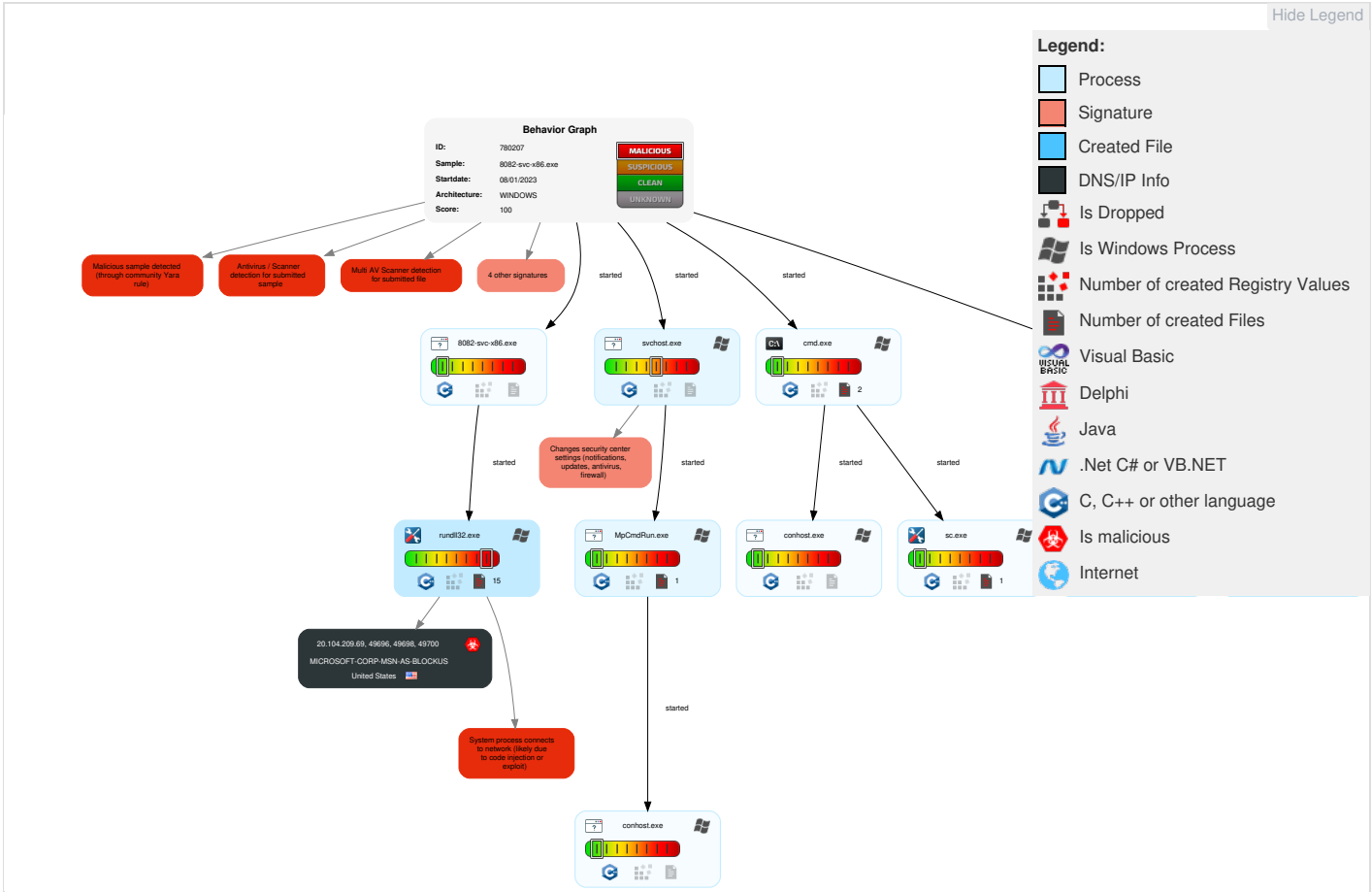
Yara detected CobaltStrike

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
2 Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Native API	2 Valid Accounts	2 Valid Accounts	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	3 Service Execution	4 Windows Service	2 1 Access Token Manipulation	2 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	4 Windows Service	1 Software Packing	NTDS	1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 1 2 Process Injection	1 DLL Side-Loading	LSA Secrets	4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Valid Accounts	DCSync	1 Process 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 Virtualization/Sandbox Evasion	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	2 1 Access Token Manipulation	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 1 2 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

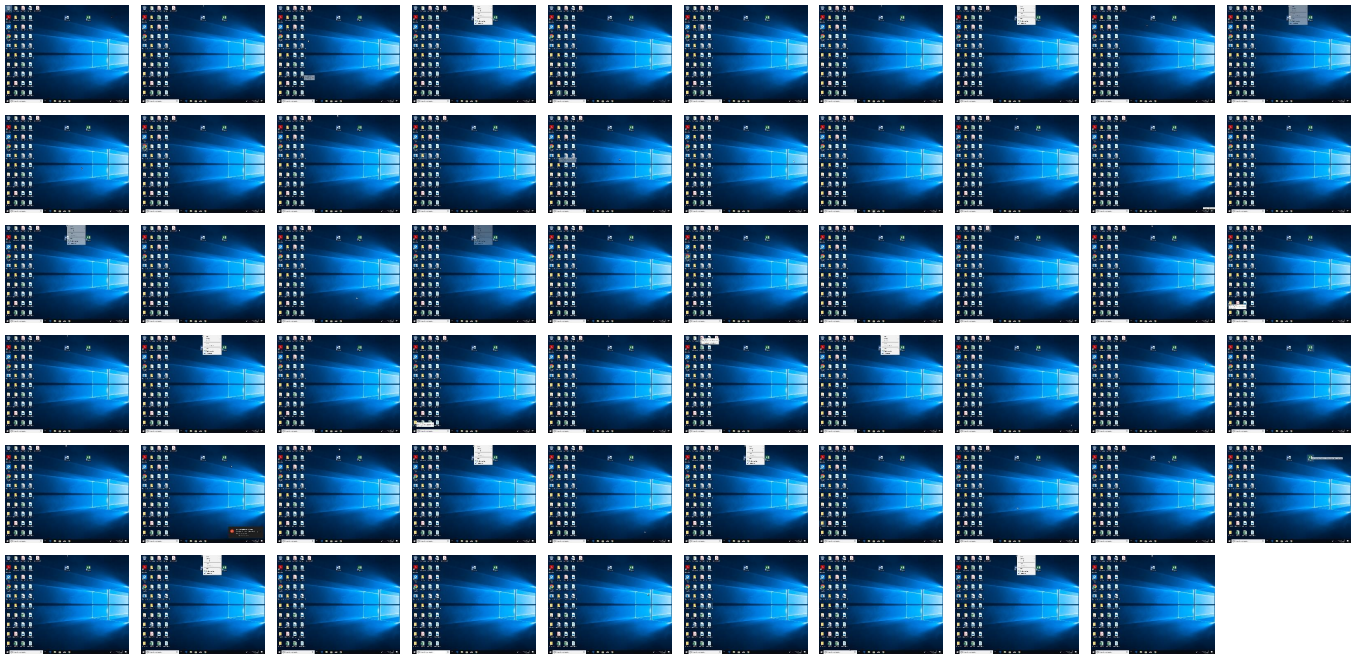
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
8082-svc-x86.exe	93%	ReversingLabs	Win32.Trojan.CobaltStrike	
8082-svc-x86.exe	79%	Virustotal		Browse
8082-svc-x86.exe	100%	Avira	TR/Crypt.XPACK.Gen	
8082-svc-x86.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.8082-svc-x86.exe.400000.0.unpack	100%	Avira	TR/Hijacker.Gen		Download File
6.0.8082-svc-x86.exe.400000.0.unpack	100%	Avira	TR/Hijacker.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://20.104.209.69:8082/broadcast	0%	Virustotal		Browse
20.104.209.69	1%	Virustotal		Browse
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prod	2%	Virustotal		Browse
20.104.209.69	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prod	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcast	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://20.104.209.69:8082/broadcast	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
20.104.209.69	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prod	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

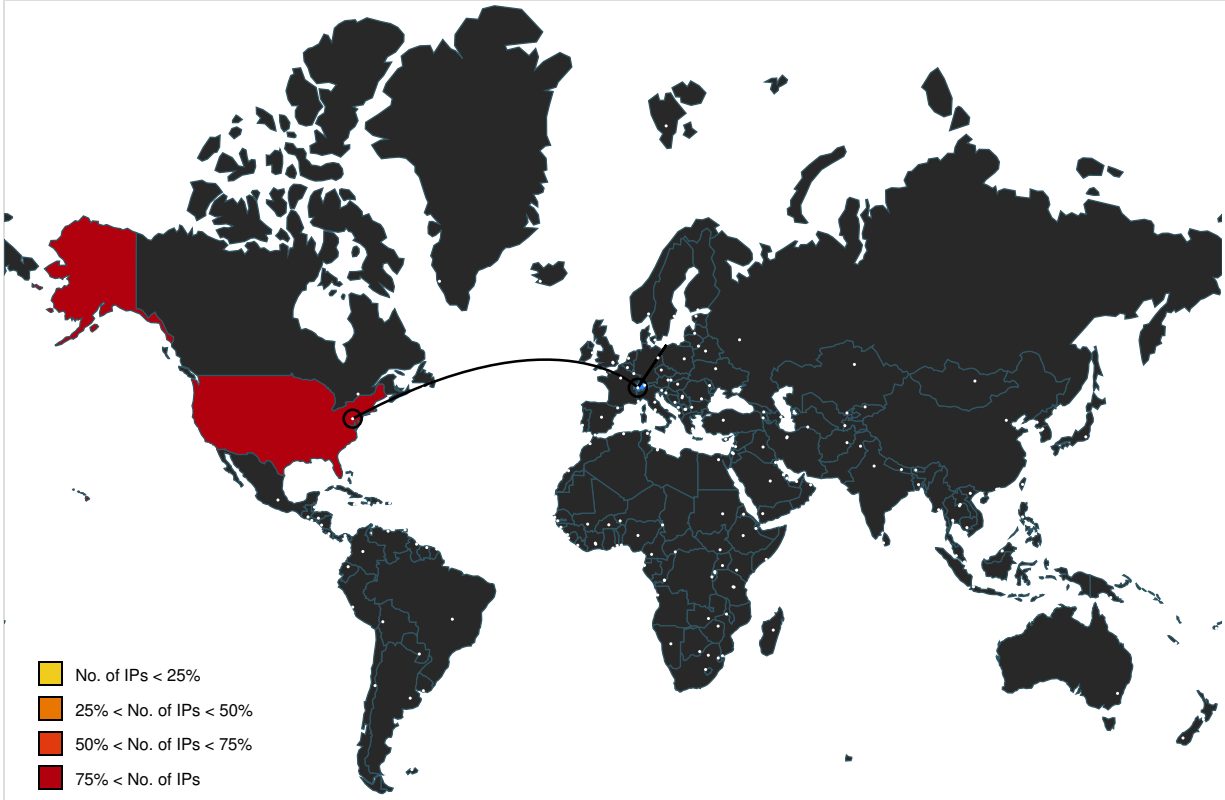
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000B.00000003.315795329.0000027921661000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000003.315845807.0000027921656000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000B.00000002.316137245.000002792163C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000B.00000003.315795329.0000027921661000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000B.00000002.316137245.000002792163C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.amazon.com	rundll32.exe, 00000007.00000002.780318528.0000000001100000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000B.00000003.315812082.000002792165A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.316173182.000002792165C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000B.00000002.316159805.000002792164D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.315774082.0000027921648000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://d22u79neyj432a.cloudfront.net/bfc50dfa-8e10-44b5-ae59-ac26bfc71489/54857e6d-c060-4b3c-914a-8	rundll32.exe, 00000007.00000002.780464664.0000000003849000.00000004.00000800.00020000.00000000.sdmp, rundll32.exe, 00000007.00000002.780479562.0000000003873000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000B.00000002.316137245.000002792163C000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000003.315832194.0000027921640000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000B.00000003.315795329.0000027921661000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000B.00000003.315832194.0000027921640000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.315812082.000002792165A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.316173182.000002792165C000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000002.316137245.000002792163C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.316062632.0000027921613000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000B.00000003.315832194.0000027921640000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.316147968.0000027921642000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.315866958.0000027921641000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000009.00000002.773656447.000001FA2D043000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	low
http:// https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000002.316159805.000002792164D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.315774082.0000027921648000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000B.00000003.315795329.0000027921661000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000003.315832194.0000027921640000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.315795329.0000027921661000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.315795329.0000027921661000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000003.315812082.000002792165A000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000B.00000003.315832194.0000027921640000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000002.316173182.000002792165C000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000003.315812082.000002792165A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.316173182.000002792165C000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000B.00000003.315832194.0000027921640000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.316147968.0000027921642000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.315866958.0000027921641000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000B.00000002.316188366.0000027921665000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.315812082.000002792165A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.315866958.0000027921641000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000B.00000003.315795329.0000027921661000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000B.00000002.316129188.000002792163A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.294187920.000002792163 1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000002.316173182.000002792165C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000009.00000002.773656447.000001FA2D043000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000B.00000002.316062632.0000027921613000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000B.00000003.315795329.0000027921661000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000002.316137245.000002792163C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000009.00000002.773656447.000001FA2D043000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000003.315812082.000002792165A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.316173182.000002792165C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000003.315812082.000002792165A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.104.209.69	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	780207
Start date and time:	2023-01-08 16:05:54 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8082-svc-x86.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run as Windows Service
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@21/3@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 41.8%) • Quality average: 28.8% • Quality standard deviation: 39.3%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:06:55	API Interceptor	536x Sleep call for process: rundll32.exe modified
16:08:14	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.1708792130630052
Encrypted:	false
SSDEEP:	192:cY+38+DJ5+inJg3+igJU+LY+XY+ntn+E5L+ME+P:j+s+j+j3+12+0+I+9+C+f+P
MD5:	310B37B81A13DA06B304769425131FF4
SHA1:	A401B6BB56A3D5CE3F55E16EB9FA08F73F897154
SHA-256:	699E8D9D93FF023D858F2FA2BF1DE3E97ECF0E62994EE28D352B6B3FF6585C41
SHA-512:	1519B3C684CBBCC647F72488690A627AE61F6B28830DAE6FE72197F5DE9DCBBF5B1FF4033B6C9EEFB8DAEDB52BCF9B6DA524BDB817DDED9D3460D7E2238A 9277
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-............-.

C:\servicereg.log

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	28
Entropy (8bit):	3.678439190827718
Encrypted:	false
SSDEEP:	3:4A4AnXjzSv:4HAnXjg
MD5:	A8F4D690C5BDE96AD275C7D4ABE0E3D3
SHA1:	7C62C96EFD2CA4F3C3EBF0B24C9B5B4C04A4570A
SHA-256:	596CCC911C1772735AAC6A6B756A76D3D55BCECD006B980CF147090B2243FA7B
SHA-512:	A875EBE3C5CDF222FF9D08576F4D996AF827A1C86B3E758CE23F6B33530D512A82CE8E39E519837512080C6212A0A19B3385809BE5F5001C4E488DD79550B852
Malicious:	false
Preview:	[SC] CreateService SUCCESS..

C:\servicestart.log

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	421

Entropy (8bit):	3.525933555991636
Encrypted:	false
SSDEEP:	6:lg3D/8FlgVKBRjGxVVLvH2s/u8qLLFmLaZnsHgm66//V+NmQWWfq:lgADgV0qVbH2suZLQqOVKmQ9q
MD5:	06C2EB35C508629EF83134977E913549
SHA1:	3F477C1C5A1FFE03C4C2D7F9C0B4215172EDDDDF
SHA-256:	A95C10E6FC6BB48D884DFAADF41CE46A958DCB47A454C4EB31156A0A835C18C7
SHA-512:	23C736B181DCA12EBD83E8DA3CA8E8C3890B275D27FE64B6954942FEF7EB0E2494736554DD6FFDA892312564BCBB17232B7A432CD03973CE9BC8A025654860E A
Malicious:	false
Preview:	..SERVICE_NAME: CfsHz .. TYPE : 10 WIN32_OWN_PROCESS .. STATE : 2 START_PENDING .. (N OT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN).. WIN32_EXIT_CODE : 0 (0x0).. SERVICE_EXIT_CODE : 0 (0x0).. CHECKPOINT : 0x0.. WAIT_HINT : 0x7d0.. PID : 1284.. FLAGS : ..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.668168868781468
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	8082-svc-x86.exe
File size:	285696
MD5:	8fc088eec229a693f2d754c67a2e506a
SHA1:	0043b6ba9f8edfd83d00bbce364797d4c65b3b75
SHA256:	deeb89a16aa2b7b63504602de422f508c196b8be3289e57f3b9d74337d585425
SHA512:	8108f5d1e8dceea2276c89b5bf964e463fe466f25e115f80bb798f83e7619e7c4b40321e695b41570cc5136bc63b2fba90f1a34e4d05949d87ccf309a9d90ee8
SSDEEP:	6144:uQJAy6O5fo59McMv/0pWHV77hLB5FPfPfPfP8DRDNpGxnT:uQN6O5w8/XVXhLB5FPfPfPfP8D9NpgnT
TLSH:	D154CF87C75D0CA2F06A3A389EE77D676A19EBE1E30E0D4ED2BB27A50D06797441C701
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^..... ...X.....0....@.....g..... .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4014b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, DEBUG_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5EDED50D [Tue Jun 9 00:17:17 2020 UTC]
TLS Callbacks:	0x401bd0, 0x401b80
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	de77f3139eaf74f1b255ab7be0b6605f

Entrypoint Preview
Instruction
sub esp, 0Ch
mov dword ptr [00447040h], 00000001h
call 00007FE1947954C3h
add esp, 0Ch
jmp 00007FE194793BABh
lea esi, dword ptr [esi+00000000h]
sub esp, 0Ch
mov dword ptr [00447040h], 00000000h
call 00007FE1947954A3h
add esp, 0Ch
jmp 00007FE194793B8Bh
nop
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
sub esp, 18h
mov eax, dword ptr [00445420h]
test eax, eax
je 00007FE194793F2Eh
mov dword ptr [esp], 00446020h
call dword ptr [004481CCh]
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007FE194793F08h
mov dword ptr [esp+04h], 0044602Eh
mov dword ptr [esp], eax
call dword ptr [004481D0h]
sub esp, 08h
mov edx, eax
test edx, edx
je 00007FE194793EFBh
mov dword ptr [esp], 00445420h
call edx
leave
ret
lea esi, dword ptr [esi+00h]
push ebp
mov ebp, esp
pop ebp
ret
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
mov ebp, esp

Instruction
sub esp, 10h
mov edx, dword ptr [0040300Ch]
mov eax, dword ptr [ebp+08h]
test edx, edx
jle 00007FE194793F12h
cmp dword ptr [00403010h], 00000000h
jle 00007FE194793F09h
mov ecx, dword ptr [004481CCh]
mov dword ptr [eax+edx], ecx
mov edx, dword ptr [000000D0h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x48000	0x8a0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x4a000	0x18	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x48180	0x130	.idata
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	0x1fd4	0x2000	False	0.563720703125	data	5.933774570860191	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x3000	0x42424	0x42600	False	0.5399489465630886	data	6.670005359968773	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x46000	0x324	0x400	False	0.4970703125	data	4.535472821564213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.bss	0x47000	0x47c	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0x48000	0x8a0	0xa00	False	0.373046875	data	4.745754334582236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x49000	0x34	0x200	False	0.068359375	Matlab v4 mat-file (little endian) `\035@, numeric, rows 4198416, columns 0	0.2655385886073115	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x4a000	0x20	0x200	False	0.05078125	data	0.22482003450968063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Imports

DLL	Import
ADVAPI32.dll	RegisterServiceCtrlHandlerA, SetServiceStatus, StartServiceCtrlDispatcherA

DLL	Import
KERNEL32.dll	CloseHandle, ConnectNamedPipe, CreateFileA, CreateNamedPipeA, CreateProcessA, CreateThread, DeleteCriticalSection, EnterCriticalSection, ExitProcess, FreeLibrary, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetEnvironmentVariableA, GetLastError, GetModuleHandleA, GetProcAddress, GetStartupInfoA, GetSystemTimeAsFileTime, GetThreadContext, GetTickCount, InitializeCriticalSection, LeaveCriticalSection, LoadLibraryA, LoadLibraryW, QueryPerformanceCounter, ReadFile, ResumeThread, SetThreadContext, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualAllocEx, VirtualProtect, VirtualProtectEx, VirtualQuery, WriteFile, WriteProcessMemory
msvcrt.dll	__dllonexit, __getmainargs, __initenv, __lconv_init, __set_app_type, __setusermatherr, _acmdln, _amsg_exit, _cexit, _fmode, _initterm, _iob, _lock, _onexit, _snprintf, _unlock, _winmajor, abort, calloc, exit, fprintf, free, fwrite, malloc, memcpy, signal, sprintf, strlen, strncmp, vfprintf

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:06:55.722184896 CET	49696	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:55.837234974 CET	8082	49696	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:55.837413073 CET	49696	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:55.838337898 CET	49696	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:55.952249050 CET	8082	49696	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:55.958020926 CET	8082	49696	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:55.958054066 CET	8082	49696	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:55.958106041 CET	49696	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:55.958148003 CET	49696	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:55.962809086 CET	8082	49696	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:55.962903023 CET	49696	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:55.967139959 CET	49696	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.081063032 CET	8082	49696	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.086762905 CET	49698	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.202558041 CET	8082	49698	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.202759981 CET	49698	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.203737020 CET	49698	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.318003893 CET	8082	49698	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.322467089 CET	8082	49698	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.322505951 CET	8082	49698	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.322594881 CET	8082	49698	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.322645903 CET	49698	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.322727919 CET	49698	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.325087070 CET	49698	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.430943966 CET	49700	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.439516068 CET	8082	49698	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.545618057 CET	8082	49700	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.545813084 CET	49700	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.546406031 CET	49700	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.660610914 CET	8082	49700	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.662009001 CET	8082	49700	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.662036896 CET	8082	49700	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.662117004 CET	49700	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.662153006 CET	49700	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.666027069 CET	49700	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.666099072 CET	49700	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.801702023 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.916044950 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:56.916241884 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:56.929686069 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.044296980 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.560909986 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.560947895 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.560967922 CET	8082	49701	20.104.209.69	192.168.2.6

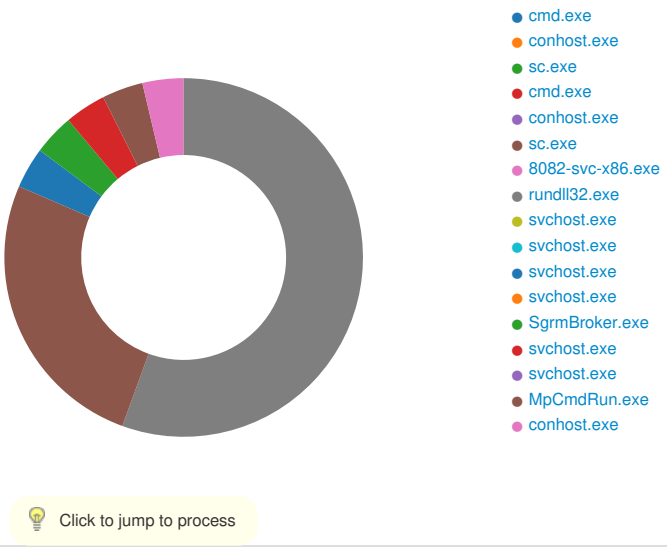
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:06:57.560990095 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.561009884 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.561029911 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.561048985 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.561068058 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.561088085 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.561106920 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.561120033 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.561177015 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.561177969 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.675915956 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.675949097 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.675968885 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.675992012 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676115036 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676131010 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676136017 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676157951 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676187038 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676193953 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676217079 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676256895 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676402092 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676424980 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676445961 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676465988 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676479101 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676487923 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676508904 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676508904 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676531076 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676548004 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676552057 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676568031 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676573992 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676597118 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676609039 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676618099 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676641941 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676652908 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.676677942 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.676709890 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.790656090 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.790764093 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.790819883 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.790863037 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.790891886 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.790904999 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.790937901 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.790952921 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.790952921 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.790973902 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.790976048 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.790999889 CET	49701	8082	192.168.2.6	20.104.209.69
Jan 8, 2023 16:06:57.791008949 CET	8082	49701	20.104.209.69	192.168.2.6
Jan 8, 2023 16:06:57.791030884 CET	49701	8082	192.168.2.6	20.104.209.69

HTTP Request Dependency Graph

- https:
  - 20.104.209.69:8082

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: **6060**, Parent PID: **1848**

General

Target ID:	0
Start time:	16:06:50
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c sc create CfsHz binpath= "C:\Users\user\Desktop\8082-svc-x86.exe" >> C:\servicereg.log 2>&1
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Analysis Process: conhost.exe PID: **6068**, Parent PID: **6060**

General

Target ID:	1
Start time:	16:06:50
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: sc.exe PID: **6100**, Parent PID: **6060**

General

Target ID:	2
Start time:	16:06:50
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc create CfsHz binpath= "C:\Users\user\Desktop\8082-svc-x86.exe"
Imagebase:	0xac0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\servicereg.log	0	28	5b 53 43 5d 20 43 72 65 61 74 65 53 65 72 76 69 63 65 20 53 55 43 43 45 53 53 0d 0a	[SC] CreateService SUCCESS	success or wait	1	ACB97A	WriteFile

Analysis Process: cmd.exe PID: **3140**, Parent PID: **1848**

General

Target ID:	3
Start time:	16:06:52
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c sc start CfsHz >> C:\servicestart.log 2>&1
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\servicestart.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1BD194	CreateFileW

Analysis Process: conhost.exe PID: **2752**, Parent PID: **3140**

General

Target ID:	4
Start time:	16:06:52
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: sc.exe PID: **988**, Parent PID: **3140**

General

Target ID:	5
Start time:	16:06:52
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc start CfsHz
Imagebase:	0xac0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\servicestart.log	0	421	0d 0a 53 45 52 56 49 43 45 5f 4e 41 4d 45 3a 20 43 66 73 48 7a 20 0d 0a 20 20 20 20 20 20 20 20 54 59 50 45 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3a 20 31 30 20 20 57 49 4e 33 32 5f 4f 57 4e 5f 50 52 4f 43 45 53 53 20 20 0d 0a 20 20 20 20 20 20 20 20 53 54 41 54 45 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3a 20 32 20 20 53 54 41 52 54 5f 50 45 4e 44 49 4e 47 20 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 28 4e 4f 54 5f 53 54 4f 50 50 41 42 4c 45 2c 20 4e 4f 54 5f 50 41 55 53 41 42 4c 45 2c 20 49 47 4e 4f 52 45 53 5f 53 48 55 54 44 4f 57 4e 29 0d 0a 20 20 20 20 20 20 20 20 57 49 4e 33 32 5f 45 58 49 54 5f 43 4f 44 45 20 20 20 20 20 3a 20 30 20 20 28 30 78 30 29 0d 0a 20 20 20 20 20 20 20 20 53	SERVICE_NAME: CfsHz TYPE : 10 WIN32_O WN_PROCESS STATE : 2 START_PENDING (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN) WIN32_EXIT_CODE : 0 (0x0) S	success or wait	1	AC5C54	WriteFile

Analysis Process: 8082-svc-x86.exe

PID: **1284**, Parent PID: **576**

General

Target ID:	6
Start time:	16:06:52
Start date:	08/01/2023
Path:	C:\Users\user\Desktop\8082-svc-x86.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\8082-svc-x86.exe
Imagebase:	0x400000
File size:	285696 bytes
MD5 hash:	8FC088EEC229A693F2D754C67A2E506A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x, Description: Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x), Source: 00000006.00000000.252641646.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: gssincla@google.com • Rule: CobaltStrike_Resources_Artifact32svc_Exe_v3_1_v3_2_v3_14_and_v4_x, Description: Cobalt Strike\'s resources/artifact32svc(big).exe signature for versions 3.1 and 3.2 (with overlap with v3.14 through v4.x), Source: 00000006.00000002.255993294.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: gssincla@google.com • Rule: CobaltStrike_Sleeve_BeaconLoader_VA_x86_o_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/BeaconLoader.VA.x86.o (VirtualAlloc) Versions 4.3 through at least 4.6, Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: Trojan_Raw_Generic_4, Description: unknown, Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: FireEye • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key., Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Metasploit_7bc0f998, Description: Identifies the API address lookup function leverage by metasploit shellcode, Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Metasploit_c9773203, Description: Identifies the 64 bit API hashing function used by Metasploit. This has been re-used by many other malware families., Source: 00000006.00000002.256178175.0000000001150000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\MSSE-8160-server	unknown	212995	success or wait	1	40196A	ReadFile

Analysis Process: rundll32.exe PID: **3128**, Parent PID: **1284**

General

Target ID:	7
Start time:	16:06:54
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\rundll32.exe
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000007.00000002.780101096.00000000010C6000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000007.00000002.780610935.0000000003DA0000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x, Description: Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x, Source: 00000007.00000002.780610935.0000000003DA0000.00000004.00000800.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: CobaltStrike_Sleeve_Beacon_Dll_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/beacon.dll Versions 4.3 and 4.4, Source: 00000007.00000002.779835594.00000000010A0000.00000020.00001000.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: CobaltStrike_Sleeve_BeaconLoader_VA_x86_o_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/BeaconLoader.VA.x86.o (VirtualAlloc) Versions 4.3 through at least 4.6, Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: Trojan_Raw_Generic_4, Description: unknown, Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: FireEye • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key., Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Metasploit_7bc0f998, Description: Identifies the API address lookup function leverage by metasploit shellcode, Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Metasploit_c9773203, Description: Identifies the 64 bit API hashing function used by Metasploit. This has been re-used by many other malware families., Source: 00000007.00000003.256646487.0000000000B40000.00000020.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Metasploit_7bc0f998, Description: Identifies the API address lookup function leverage by metasploit shellcode, Source: 00000007.00000002.780169919.00000000010D2000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Metasploit_c9773203, Description: Identifies the 64 bit API hashing function used by Metasploit. This has been re-used by many other malware families., Source: 00000007.00000002.780169919.00000000010D2000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10A1384	HttpSendRequestA
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History\History.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10A1384	HttpSendRequestA

Analysis Process: svchost.exe PID: **2392**, Parent PID: **576**

General	
Target ID:	8
Start time:	16:07:08
Start date:	08/01/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5416**, Parent PID: **576**

General	
Target ID:	9
Start time:	16:07:10
Start date:	08/01/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
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: svchost.exe PID: **4532**, Parent PID: **576**

General	
Target ID:	10
Start time:	16:07:11
Start date:	08/01/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5644**, Parent PID: **576**

General

Target ID:	11
Start time:	16:07:11
Start date:	08/01/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: **4380**, Parent PID: **576**

General

Target ID:	12
Start time:	16:07:12
Start date:	08/01/2023
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff689cb0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **4792**, Parent PID: **576**

General

Target ID:	13
Start time:	16:07:12
Start date:	08/01/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

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

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5932**, Parent PID: **576**

General

Target ID:	14
Start time:	16:07:13
Start date:	08/01/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: **5448**, Parent PID: **5932**

General

Target ID:	15
Start time:	16:08:13
Start date:	08/01/2023
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff604670000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written								
File Path	**Offset**	**Length**	**Value**	**Ascii**	**Completion**	**Count**	**Source Address**	**Symbol**
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF60469BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4a 00 61 00 6e 00 20 00 0e 20 30 00 38 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 31 00 36 00 3a 00 30 00 38 00 3a 00 31 00 34 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sun Jan 08 2023 16:08:14	success or wait	1	7FF60469BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF60469BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF60469BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF60469BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4a 00 61 00 6e 00 20 00 0e 20 30 00 38 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 31 00 36 00 3a 00 30 00 38 00 3a 00 31 00 34 00 0d 00 0a 00	MpCmdRun: End Time: Sun Jan 08 2023 16:08:14	success or wait	1	7FF60469BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF60469BC96	WriteFile

Analysis Process: conhost.exe PID: **5512**, Parent PID: **5448**

General

Target ID:	16
Start time:	16:08:13
Start date:	08/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly