ID: 780212
Sample Name: 8082-svc-x64.exe
Cookbook: default.jbs
Time: 16:11:04
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

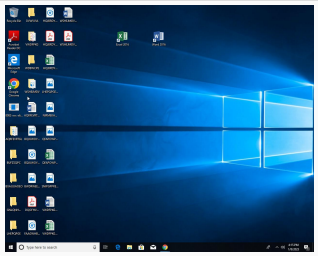
Windows Analysis Report

8082-svc-x64.exe

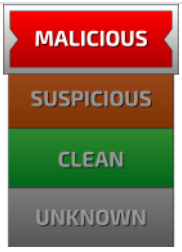
Overview

General Information

Sample Name:	8082-svc-x64.exe
Analysis ID:	780212
MD5:	89be3be20ca0dc..
SHA1:	4f92b6f168ee853.
SHA256:	37e828da01820a.
Tags:	45139105143 exe opendir
Infos:	



Detection



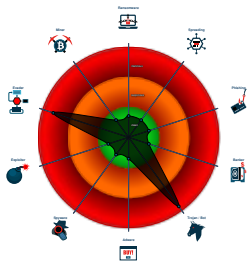
CobaltStrike

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
- Query firmware table information (lik…
- Uses known network protocols on n…
- Changes security center settings (n…
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Modifies the context of a thread in a…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 4696 cmdline: cmd /c sc create qFrdg binpath= "C:\Users\user\Desktop\8082-svc-x64.exe" >> C:\servicereg.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 5368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 5296 cmdline: sc create qFrdg binpath= "C:\Users\user\Desktop\8082-svc-x64.exe" MD5: 24A3E2603E63BCB9695A2935D3B24695)
- cmd.exe (PID: 5280 cmdline: cmd /c sc start qFrdg >> C:\servicestart.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 5208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - sc.exe (PID: 588 cmdline: sc start qFrdg MD5: 24A3E2603E63BCB9695A2935D3B24695)
- 8082-svc-x64.exe (PID: 4044 cmdline: C:\Users\user\Desktop\8082-svc-x64.exe MD5: 89BE3BE20CA0DCE73C12A5A015BCB9A5)
  - rundll32.exe (PID: 3988 cmdline: C:\Windows\System32\rundll32.exe MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 2292 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3112 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5384 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5320 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5648 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1844 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5280 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3548 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5628 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 496 cmdline: c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **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-x64.exe	CobaltStrike_Resources_Artifact64_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact64{.exe,.dll,svc.exe,svcbig.exe,big.exe,big.dll,.x64.dll,big.x64.dll} and resource/artifactuac(alt)64.exe signature for versions v3.14 through v4.x	gssincla@google.com	• 0xd75:$fmtBuilder: 41 B8 5C 00 00 00 C7 44 24 50 5C 00 00 00 C7 44 24 48 65 00 00 00 C7 44 24 40 70 00 00 00 C7 44 24 38 69 00 00 00 C7 44 24 30 70 00 00 00 C7 44 24 28 5C 00 00 00 C7 44 24 20 2E 00 00 00 89 54 ... • 0x44e50:$fmtString: %c%c%c%c%c%c%c%cMSSE-%d-server
8082-svc-x64.exe	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.sdmp	SUSP_PS1_FromBase64String_Content_Indicator	Detects suspicious base64 encoded PowerShell expressions	Florian Roth	• 0xdfd8:$: ::FromBase64String("H4s • 0xdfd8:$: ::FromBase64String("H4sIA

Source	Rule	Description	Author	Strings
00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.sdmp	CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x	Cobalt Strike\'s resources/cmd.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x	gssincla@google.com	• 0xdfb0:$ps1: $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(• 0x36eb9:$ps2:));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
00000007.00000003.258338449.00000270F7ECF000.00000004.00001000.00020000.00000000.sdmp	SUSP_PS1_FromBase64String_Content_Indicator	Detects suspicious base64 encoded PowerShell expressions	Florian Roth	• 0xdfd8:$: ::FromBase64String("H4s • 0xdfd8:$: ::FromBase64String("H4sIA
00000007.00000003.258338449.00000270F7ECF000.00000004.00001000.00020000.00000000.sdmp	CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x	Cobalt Strike\'s resources/cmd.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x	gssincla@google.com	• 0xdfb0:$ps1: $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(• 0x36eb9:$ps2:));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
00000007.00000003.259556470.00000270F7ECF000.00000004.00001000.00020000.00000000.sdmp	SUSP_PS1_FromBase64String_Content_Indicator	Detects suspicious base64 encoded PowerShell expressions	Florian Roth	• 0xdfd8:$: ::FromBase64String("H4s • 0xdfd8:$: ::FromBase64String("H4sIA
Click to see the 36 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.8082-svc-x64.exe.400000.0.unpack	CobaltStrike_Resources_Artifact64_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact64{.exe,.dll,svc.exe,svcbig.exe,big.exe,big.dll,.x64.dll,big.x64.dll} and resource/artifactuac(alt)64.exe signature for versions v3.14 through v4.x	gssincla@google.com	• 0xd75:$fmtBuilder: 41 B8 5C 00 00 00 C7 44 24 50 5C 00 00 00 C7 44 24 48 65 00 00 00 C7 44 24 40 70 00 00 00 C7 44 24 38 69 00 00 00 C7 44 24 30 70 00 00 00 C7 44 24 28 5C 00 00 00 C7 44 24 20 2E 00 00 00 89 54 ... • 0x44e50:$fmtString: %c%c%c%c%c%c%c%cMSSE-%d-server
6.2.8082-svc-x64.exe.400000.0.unpack	CobaltStrike_Resources_Artifact64_v3_14_to_v4_x	Cobalt Strike\'s resources/artifact64{.exe,.dll,svc.exe,svcbig.exe,big.exe,big.dll,.x64.dll,big.x64.dll} and resource/artifactuac(alt)64.exe signature for versions v3.14 through v4.x	gssincla@google.com	• 0xd75:$fmtBuilder: 41 B8 5C 00 00 00 C7 44 24 50 5C 00 00 00 C7 44 24 48 65 00 00 00 C7 44 24 40 70 00 00 00 C7 44 24 38 69 00 00 00 C7 44 24 30 70 00 00 00 C7 44 24 28 5C 00 00 00 C7 44 24 20 2E 00 00 00 89 54 ... • 0x44e50:$fmtString: %c%c%c%c%c%c%c%cMSSE-%d-server
6.0.8082-svc-x64.exe.400000.0.unpack	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	
6.2.8082-svc-x64.exe.400000.0.unpack	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	

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

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Anti Debugging

Found API chain indicative of debugger detection

HIPS / PFW / Operating System Protection Evasion

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

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

Lowering of HIPS / PFW / Operating System Security Settings

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

Remote Access Functionality

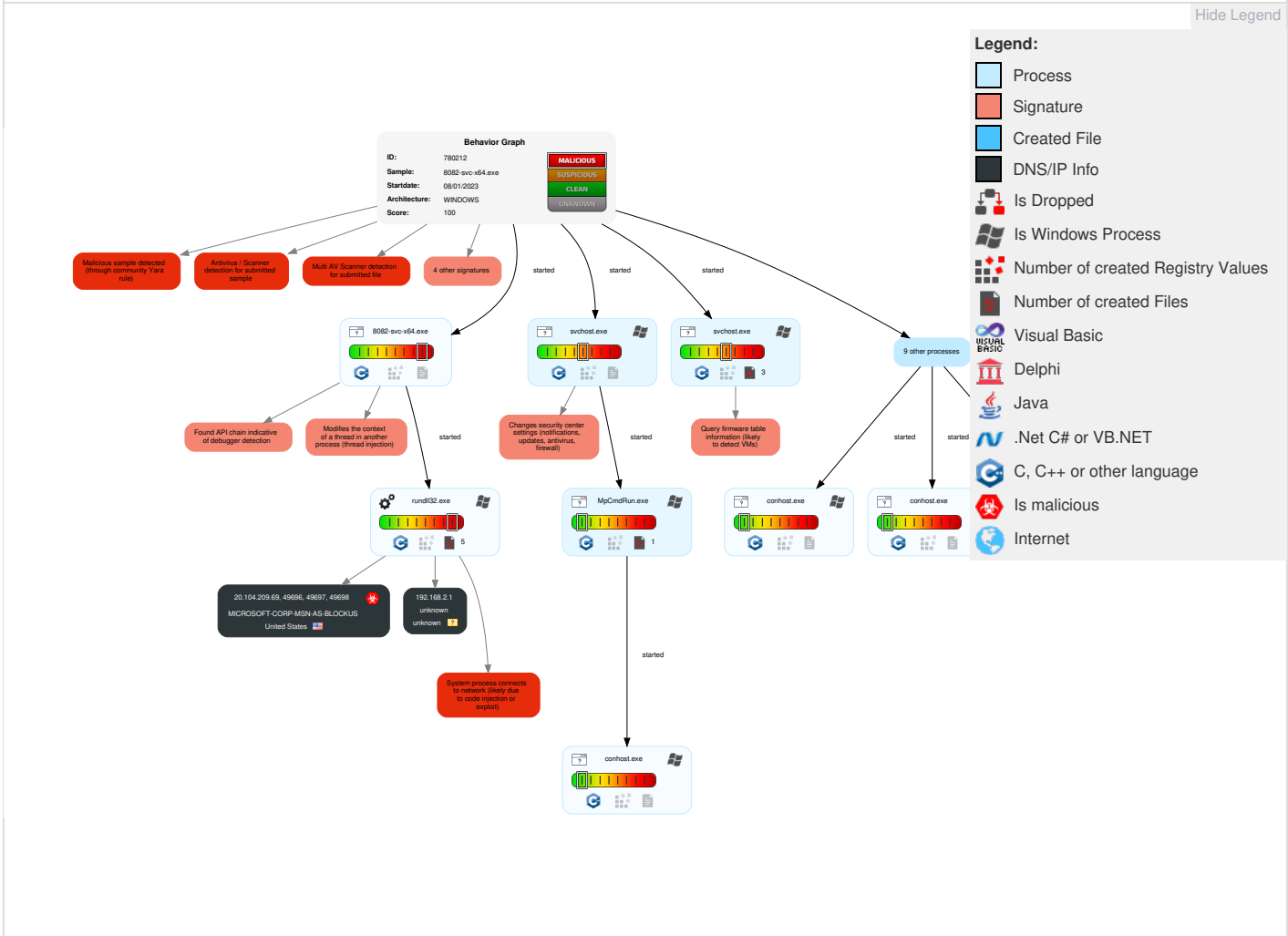
Yara detected CobaltStrike

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
Valid Accounts	1 Windows Management Instrumentation	4 Windows Service	4 Windows Service	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Service Execution	1 DLL Side-Loading	2 1 2 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 3 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	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)	2 1 2 Process Injection	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System 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	System Owner/User 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	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

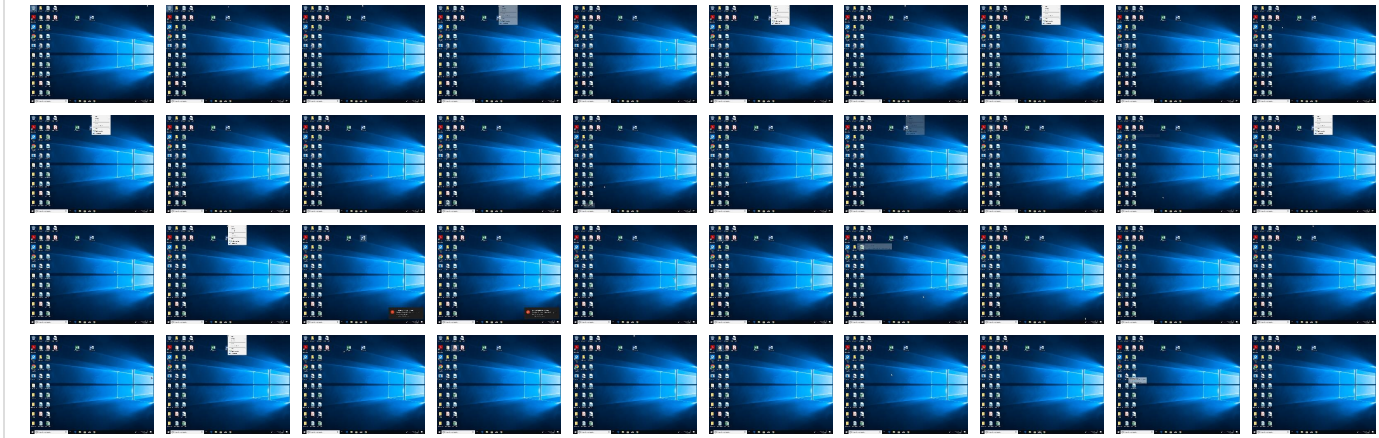
Behavior Graph



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-x64.exe	80%	ReversingLabs	Win64.Backdoor.CobaltStrike	
8082-svc-x64.exe	68%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
8082-svc-x64.exe	100%	Avira	HEUR/AGEN.1202022	
8082-svc-x64.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://20.104.209.69:8082/broadcastgZ	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcastsi	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcast	0%	Virustotal		Browse
20.104.209.69	1%	Virustotal		Browse
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prodMicrosoft	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prodf5	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prodQ	0%	Avira URL Cloud	safe	
20.104.209.69	0%	Avira URL Cloud	safe	
http://https://www.amazon.comL	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/broadcastashSessionKeyBackward	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcast	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://20.104.209.69:8082/broadcastashSessionKeyBackwardQ	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcast%bT	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcastashSessionKeyBackwardY	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcastp	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcastashSessionKeyBackwarda	0%	Avira URL Cloud	safe	
http://https://www.amazon.compN	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prodE?b	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcastashSessionKeyBackwardp	0%	Avira URL Cloud	safe	
http://20.104.209.69:8082/broadcastwe	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	• Avira URL Cloud: safe	unknown

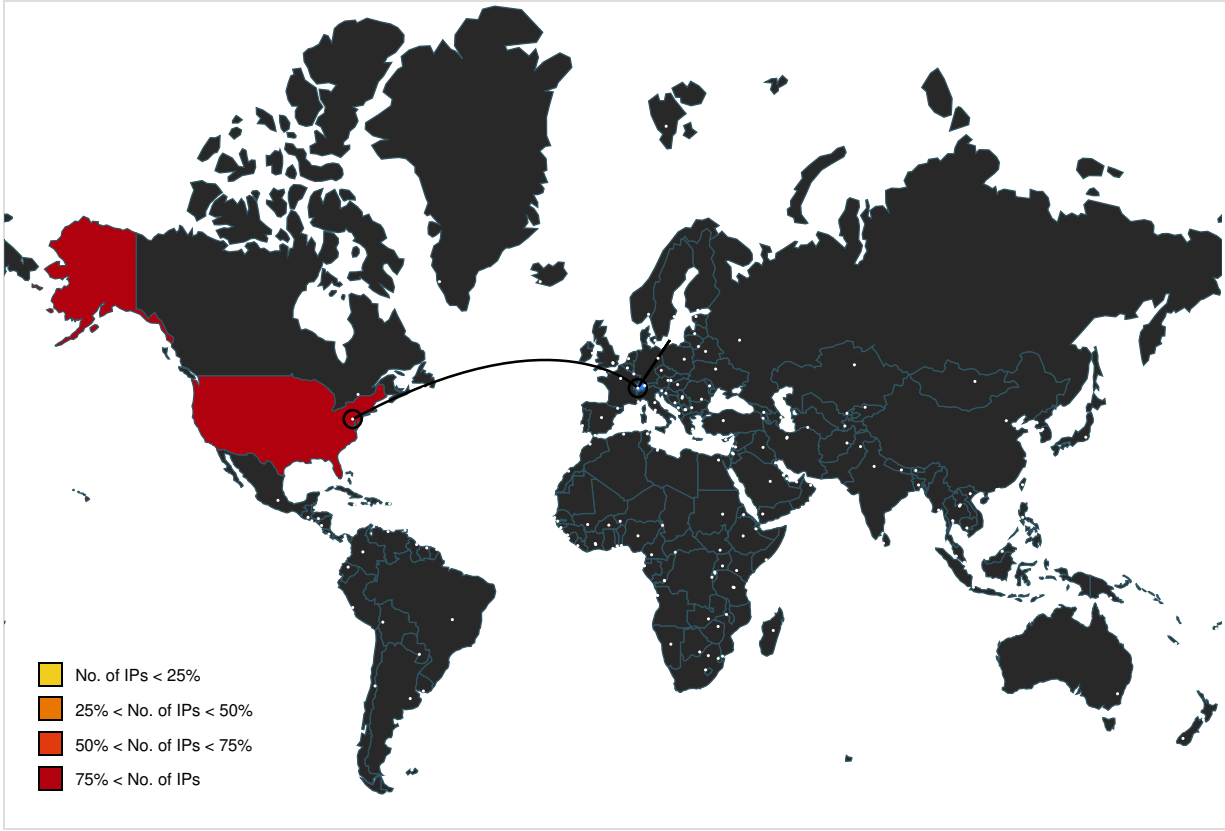
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://20.104.209.69:8082/broadcastsi	rundll32.exe, 00000007.00000002.77202132 0.00000270F7ECF000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://20.104.209.69:8082/broadcastgZ	rundll32.exe, 00000007.00000002.77161674 8.00000270F7E7B000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000C.00000002.314969937 .0000020E99E3C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000C.00000003.314657698 .0000020E99E61000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen .ashx	svchost.exe, 0000000C.00000002.314969937 .0000020E99E3C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.amazon.com	rundll32.exe, 00000007.00000002.77185823 6.00000270F7EB3000.00000004.00000001.000 20000.00000000.sdmp	false		high
http:// https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000C.00000002.314999790 .0000020E99E5C000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 C.00000003.314677423.0000020E99E5A000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000C.00000002.314988771 .0000020E99E4D000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 C.00000003.314626551.0000020E99E47000.00 000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000C.00000003.314657698 .0000020E99E61000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// 20.104.209.69:8082/broadcastashSessionKeyBackward	rundll32.exe, 00000007.00000002.77202132 0.00000270F7ECF000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000C.00000002.314978785 .0000020E99E42000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 C.00000003.314715717.0000020E99E41000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314696611 .0000020E99E40000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000C.00000003.314657698 .0000020E99E61000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000C.00000003.314677423 .0000020E99E5A000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000C.00000003.314696611 .0000020E99E40000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000C.00000002.314978785 .0000020E99E42000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 C.00000003.314715717.0000020E99E41000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314696611 .0000020E99E40000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// 20.104.209.69:8082/1/events/com.amazon.csm.csa.prodMicrosoft	rundll32.exe, 00000007.00000002.77202132 0.00000270F7ECF000.00000004.00000001.000 20000.00000000.sdmp, rundll32.exe, 00000 007.00000003.259556470.00000270F7ECF000. 00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// 20.104.209.69:8082/1/events/com.amazon.csm.csa.prodf5	rundll32.exe, 00000007.00000003.25954169 1.00000270F7EC1000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.amazon.comL	rundll32.exe, 00000007.00000003.31887937 6.00000270F7F34000.00000004.00000001.000 20000.00000000.sdmp, rundll32.exe, 00000 007.00000003.507229697.00000270F7F34000. 00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 0000000C.00000002.314897356 .0000020E99E13000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000C.00000002.314969937.0000020E99E3C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prodQ	rundll32.exe, 00000007.00000003.25955647.00000270F7ECF000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000C.00000003.314657698.0000020E99E61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://20.104.209.69:8082/broadcast%bT	rundll32.exe, 00000007.00000002.771858236.00000270F7EB3000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://20.104.209.69:8082/broadcastashSessionKeyBackwardQ	rundll32.exe, 00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000C.00000003.314710088.0000020E99E56000.00000004.00000020.00020000.00000000.sdmp	false		high
http://20.104.209.69:8082/broadcastashSessionKeyBackwardY	rundll32.exe, 00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://d22u79neyj432a.cloudfront.net/bfc50dfa-8e10-44b5-ae59-ac26bfc71489/54857e6d-c060-4b3c-914a-8	rundll32.exe, 00000007.00000003.507353227.00000270F7F2C000.00000004.00001000.00020000.00000000.sdmp, rundll32.exe, 00000007.00000002.772830402.00000270F81A2000.00000004.00001000.00020000.00000000.sdmp, rundll32.exe, 00000007.00000002.772850422.00000270F81CC000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000C.00000002.314969937.0000020E99E3C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000C.00000003.314696611.0000020E99E40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000C.00000002.314999790.0000020E99E5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314677423.0000020E99E5A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314696611.0000020E99E40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://20.104.209.69:8082/broadcastashSessionKeyBackwarda	rundll32.exe, 00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://20.104.209.69:8082/broadcastp	rundll32.exe, 00000007.00000002.771858236.00000270F7EB3000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000C.00000002.314969937.0000020E99E3C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000002.314897356.0000020E99E13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.amazon.compN	rundll32.exe, 00000007.00000003.507229697.00000270F7F34000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://%s.xboxlive.com	svchost.exe, 0000000A.00000002.772016953.000001EFB3A3E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000C.00000002.314988771.0000020E99E4D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314626551.0000020E99E47000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000C.00000003.314657698.0000020E99E61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000C.00000003.314696611.0000020E99E40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000C.00000003.314657698.0000020E99E61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://20.104.209.69:8082/broadcastashSessionKeyBackwardp	rundll32.exe, 00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000C.00000002.314999790.0000020E99E5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314677423.0000020E99E5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000C.00000002.314999790.0000020E99E5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314677423.0000020E99E5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000C.00000002.315005980.0000020E99E62000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prodE?b	rundll32.exe, 00000007.00000003.259531287.00000270F7EB7000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://20.104.209.69:8082/broadcastashSessionKeyBackwardy	rundll32.exe, 00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.sdmp	false		unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000C.00000003.314657698.0000020E99E61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000C.00000002.314963953.0000020E99E3A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.293058264.0000020E99E31000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000C.00000002.314999790.0000020E99E5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314677423.0000020E99E5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://20.104.209.69:8082/broadcastwe	rundll32.exe, 00000007.00000003.259531287.00000270F7EB7000.00000004.00001000.00020000.00000000.sdmp, rundll32.exe, 00000007.00000003.258407604.00000270F7EB7000.00000004.00001000.00020000.00000000.sdmp, rundll32.exe, 00000007.00000002.771858236.00000270F7EB3000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://activity.windows.com	svchost.exe, 0000000A.00000002.772016953.000001EFB3A3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000C.00000003.314657698.0000020E99E61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000A.00000002.772016953.000001EFB3A3E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000C.00000002.314999790.0000020E99E5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000C.00000003.314677423.0000020E99E5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000C.00000003.314677423.0000020E99E5A000.00000004.00000020.00020000.00000000.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	780212
Start date and time:	2023-01-08 16:11:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8082-svc-x64.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:	22
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@23/6@0/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 94.4% (good quality ratio 57.7%) • Quality average: 47% • Quality standard deviation: 42.5%
HCA Information:	• Successful, ratio: 86% • 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): audiodg.exe, WMIADAP.exe, backgroundTaskHost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Execution Graph export aborted for target rundll32.exe, PID 3988 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:12:02	API Interceptor	574x Sleep call for process: rundll32.exe modified
16:13:23	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:\ProgramData\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines (2494), with no line terminators
Category:	dropped

Size (bytes):	2494
Entropy (8bit):	5.238902533654171
Encrypted:	false
SSDEEP:	48:cAn/TLtfGgzmQLeUp/B8HbaSkC9+TLvps:pTLtf9zmQWkvs
MD5:	4DF7B73165FDB3306BF37443D9F45DD9
SHA1:	A4C622B53BD484692A94595CBE5BDA37E7364024
SHA-256:	B38866F06E7607504003C8C02730C11DC164FFC5D5A410EF8BAD513A0FC6A34C
SHA-512:	82F1D3D77B41773FEBD4819200EAC920494CC9C9B254296DC455DB29EA41DBB2D9910F44A692E19AFC1F8197D59C0165DB130C26B2CEAF4F1ACEF58915E618 2
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService d ataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataTyp e="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399969272148706</FirstScanAttempt Time><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399969272304939</LastMeteredScanTime><LastScanAttemptTime dataType ="21">132399969272148706</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType ="21">133051593686244000</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines (2494), with no line terminators
Category:	modified
Size (bytes):	2494
Entropy (8bit):	5.238902533654171
Encrypted:	false
SSDEEP:	48:cAn/TLtfGgzmQLeUp/B8HbaSkC9+TLvps:pTLtf9zmQWkvs
MD5:	4DF7B73165FDB3306BF37443D9F45DD9
SHA1:	A4C622B53BD484692A94595CBE5BDA37E7364024
SHA-256:	B38866F06E7607504003C8C02730C11DC164FFC5D5A410EF8BAD513A0FC6A34C
SHA-512:	82F1D3D77B41773FEBD4819200EAC920494CC9C9B254296DC455DB29EA41DBB2D9910F44A692E19AFC1F8197D59C0165DB130C26B2CEAF4F1ACEF58915E618 2
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService d ataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataTyp e="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399969272148706</FirstScanAttempt Time><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399969272304939</LastMeteredScanTime><LastScanAttemptTime dataType ="21">132399969272148706</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType ="21">133051593686244000</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\Windows\Logs\waasmedic\waasmedic.20230109_001222_097.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.739836765001473
Encrypted:	false
SSDEEP:	48:e1tr52Qzwdb7kUwdb7kE7b7klkb7kNb7kbll9l3b7k0tplwb7keb7k2b7kwub7k4:O210UK000u0N0U9J0Clw0e020B09O
MD5:	6B18F5B8FFA882DBFA70E08F9FE75B87
SHA1:	583A96633A9568C739C579AD2A17963F0C2E15B9
SHA-256:	68057E15894D024F8F5693AFCB091B8D6DC9C32DD672AA1607B73A587DE5934A
SHA-512:	11E69D25C811A66139574E0394B2CB55F3C742D713AB822C561ADD0CB7861F6C601E7CAF0E91C847C97371D3BB11DC70958D7125F9F348E9DA8C6AACC7D5D8 3
Malicious:	false
Preview:	.....l.....p.....B.....d.?/.#..Zb..... .....@.t.z.r.e.s...d.l.l.,-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,-.2.1.1.....WW..... .....j..#.....E.C.C.B.1.7.5.F.-.1.E.B.2.-.4.3.D.A.-.B.F.B.5.-.A.8.D.5.8.A.4.0.A.4.D.7...C. :.\.W.i.n.d.o.w.s.\.l.o.g.s.\.w.a.a.s.m.e.d.i.c.\.w.a.a.s.m.e.d.i.c...2.0.2.3.0.1.0.9._.0.0.1.2.2.2._.0.9.7...e.t.l.....P.P.p.....9. B.....17134.1.amd64fre.rs4_release.180410-1804.....5.@.....OYo."(.s..O.....WaaSMedicSvc.pdb..... .....

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):	10874

Entropy (8bit):	3.1652720923341064
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z5+6I3+zJm+x:j+s+v+b+P+m+0+Q+q+q+73+zk+x
MD5:	17115AC568BC54C6A57E674B9FAAFC84
SHA1:	154645C02598A224FBF5E6D9C60E9BB7629C8045
SHA-256:	6D8F8B111EDC385B817F390B3A241622BD401E5495D0A5BB0D511CBB57E80A5A
SHA-512:	C320D0B7930FDA44ED0697DF80250DF9261ECECD68E47EA96BC598F32E0A937D1CBEDEEB511CA2E99F030FDC418281E3E024024A1853CE8C0F727A87AEE14 0C
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):	3.5238386648644693
Encrypted:	false
SSDEEP:	6:lg3D/8F8B+gVKBRjGxVVLvH2s/u8qLLFmLaZnsHgm66//V+Nmmvufq:lgA2B+gV0qVbH2suZLQqOVKmrq
MD5:	96CE446762BF9C567ACF319E57B24F2C
SHA1:	5F28BC306F661968D8D43A47C629B5619DACB98B
SHA-256:	5CEC0B429C3C4F459BFC451B0F69EA008C283F7E0B5EA63228F5A77832551DE7
SHA-512:	35F5230436F8E01237C314072FBB001AE6991603BB6B573DB19ACC5D476D7D44326818D4FBBB3FD274243B7E7D8DFE41F7AD4E52AACCF315A94944F96D9DC2 0
Malicious:	false
Preview:	..SERVICE_NAME: qFrdg .. TYPE : 10 WIN32_OWN_PROCESS .. STATE : 2 START_PENDING .. (NOT_STOPPAB LE, NOT_PAUSABLE, IGNORES_SHUTDOWN).. WIN32_EXIT_CODE : 0 (0x0).. SERVICE_EXIT_CODE : 0 (0x0).. CHECKPOINT : 0x0.. WAIT_HINT : 0x7d0.. PID : 4044.. FLAGS : ..

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.355879244825435
TrID:	• Win64 Executable (generic) (12005/4) 74.80% • Generic Win/DOS Executable (2004/3) 12.49% • DOS Executable Generic (2002/1) 12.47% • VXD Driver (31/22) 0.19% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	8082-svc-x64.exe
File size:	289280

MD5:	89be3be20ca0dce73c12a5a015bcb9a5
SHA1:	4f92b6f168ee8536278fa58a6df5c9b368421030
SHA256:	37e828da01820aad58414d0b73c935a0e408c274cdd872cbbae25f9cbcba0b08
SHA512:	d8490691ad53b026586dad57bb8bc59c8c3c7c9433305d317ad9aa203d9998b4fcf0e514cc562285565a1763dca7f96cfc0c62336a98cea62026dc114908b8a7
SSDEEP:	6144:6p2TnO+/tCo4wsn5PO/ziUZmUhS6b2m+7HUDnivKMpurzC37gmdqDqq7rvxAiS7Y:6onVGia9dqD5uO6lW
TLSH:	4654BF0AE855E917CB4DE07857630F7A27FB9FFEC42519A6313944236F9BA3B98C5200
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....^...../.....$...B.....@.....:..... .....

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, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5EDED518 [Tue Jun 9 00:17:28 2020 UTC]
TLS Callbacks:	0x401af0
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:	bed5688a4a2b5ea6984115b458755e90

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
mov dword ptr [00048BB2h], 00000001h
call 00007FB87D02CDD2h
call 00007FB87D02B24Dh
nop
nop
dec eax
add esp, 28h
ret
nop
dec eax
sub esp, 28h
mov dword ptr [00048B92h], 00000000h
call 00007FB87D02CDB2h
call 00007FB87D02B22Dh
nop
nop
dec eax
add esp, 28h
ret
nop

Instruction
dec eax
sub esp, 18h
mov eax, dword ptr [00002B12h]
test eax, eax
jle 00007FB87D02B5BAh
cmp dword ptr [00002B0Bh], 00000000h
jle 00007FB87D02B5B1h
dec eax
mov edx, dword ptr [00049E42h]
dec eax
cwde
dec eax
mov dword ptr [ecx+eax], edx
dec eax
arpl word ptr [00002AF5h], ax
dec eax
mov edx, dword ptr [00049E36h]
dec eax
mov dword ptr [ecx+eax], edx
dec eax
add esp, 18h
ret
push ebx
dec eax
sub esp, 00000500h
dec eax
mov ebx, dword ptr [edx+08h]
mov dword ptr [esp+60h], 00100002h
dec esp
mov dword ptr [esp+28h], eax
dec eax
lea edx, dword ptr [esp+30h]
dec eax
mov ecx, ebx
call dword ptr [00049E1Eh]
test eax, eax
dec esp
mov eax, dword ptr [esp+28h]
je 00007FB87D02B5B6h
dec esp
mov dword ptr [esp+000000B0h], eax
dec eax
lea edx, dword ptr [esp+30h]
dec eax
mov ecx, ebx
call dword ptr [00049E5Fh]
test eax, eax
je 00007FB87D02B59Ch
dec eax
mov ecx, ebx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4b000	0xb74	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x48000	0x2ac	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x4d000	0x28	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4b2c0	0x270	.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	0x2400	0x2400	False	0.5936414930555556	data	6.129764070813093	IMAGE_SCN_CNT_CODE, 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
.data	0x4000	0x42490	0x42600	False	0.6019781367702448	data	7.3657766804633775	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_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x47000	0x310	0x400	False	0.4541015625	data	4.1965610649629825	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_READ
.pdata	0x48000	0x2ac	0x400	False	0.3740234375	data	3.1610117624320244	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
.xdata	0x49000	0x268	0x400	False	0.2587890625	data	2.847508632820401	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.bss	0x4a000	0xa60	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
.idata	0x4b000	0xb74	0xc00	False	0.3372395833333333	data	4.3479190304641575	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	0x4c000	0x68	0x200	False	0.0703125	data	0.2694448386073115	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, 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
.tls	0x4d000	0x48	0x200	False	0.052734375	data	0.21776995545804623	IMAGE_SCN_CNT_INITIALIZED_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

Imports

DLL	Import
ADVAPI32.dll	RegisterServiceCtrlHandlerA, SetServiceStatus, StartServiceCtrlDispatcherA
KERNEL32.dll	CloseHandle, ConnectNamedPipe, CreateFileA, CreateNamedPipeA, CreateProcessA, CreateThread, DeleteCriticalSection, EnterCriticalSection, ExitProcess, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetEnvironmentVariableA, GetLastError, GetModuleHandleA, GetProcAddress, GetStartupInfoA, GetSystemTimeAsFileTime, GetThreadContext, GetTickCount, InitializeCriticalSection, LeaveCriticalSection, LoadLibraryW, QueryPerformanceCounter, ReadFile, ResumeThread, RtlAddFunctionTable, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, SetThreadContext, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualAllocEx, VirtualProtect, VirtualProtectEx, VirtualQuery, WriteFile, WriteProcessMemory
msvcrt.dll	__C_specific_handler, __dllonexit, __getmainargs, __initenv, __iob_func, __lconv_init, __set_app_type, __setusermatherr, _acmdln, _amsg_exit, _cexit, _fmode, _initterm, _lock, _onexit, _snprintf, _unlock, 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 16:12:02.749514103 CET	49696	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:02.863886118 CET	8082	49696	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:02.864079952 CET	49696	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:02.864835978 CET	49696	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:02.979211092 CET	8082	49696	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:02.983711958 CET	8082	49696	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:02.983747005 CET	8082	49696	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:02.983792067 CET	8082	49696	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:02.983789921 CET	49696	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:02.983830929 CET	49696	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:02.983830929 CET	49696	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:02.984179974 CET	49696	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.097527027 CET	49697	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.098475933 CET	8082	49696	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.212054014 CET	8082	49697	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.212165117 CET	49697	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.212759972 CET	49697	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.326652050 CET	8082	49697	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.332359076 CET	8082	49697	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.332395077 CET	8082	49697	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.332417011 CET	8082	49697	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.332514048 CET	49697	8082	192.168.2.3	20.104.209.69

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:12:03.332562923 CET	49697	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.333477020 CET	49697	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.359814882 CET	49698	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.447307110 CET	8082	49697	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.474181890 CET	8082	49698	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.474359035 CET	49698	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.487334967 CET	49698	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.601444960 CET	8082	49698	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.602344036 CET	8082	49698	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.602365017 CET	8082	49698	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.602473021 CET	49698	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.602684975 CET	49698	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.602740049 CET	49698	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.726802111 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.841469049 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.841770887 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.842420101 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.956772089 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975456953 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975534916 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975580931 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975625992 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975670099 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975671053 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.975671053 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.975718021 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975750923 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.975769043 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975775003 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.975831985 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.975836039 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975903988 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.975904942 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975972891 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:03.975991964 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:03.976028919 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090408087 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090517044 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090562105 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090636015 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090670109 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090735912 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090779066 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090814114 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090809107 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090809107 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090809107 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090809107 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090810061 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090850115 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090883017 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090889931 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090889931 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090889931 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090919018 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090943098 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090951920 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.090970993 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.090985060 CET	8082	49699	20.104.209.69	192.168.2.3

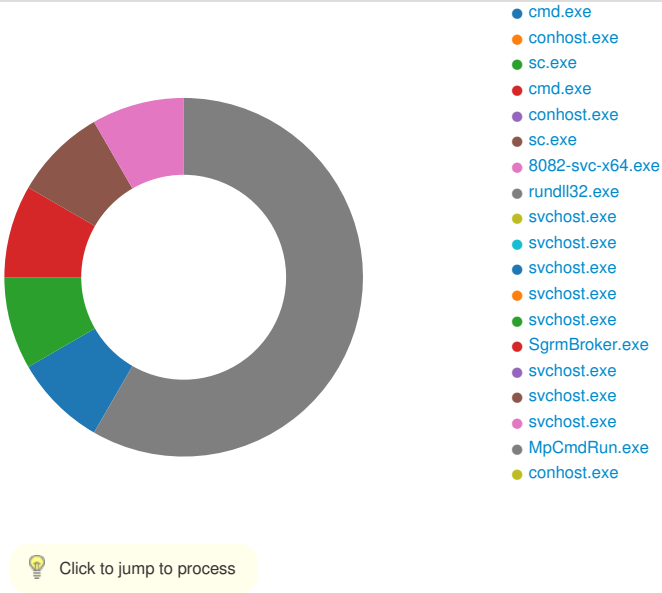
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:12:04.090995073 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.091017008 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.091048956 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.091052055 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.091075897 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.091087103 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.091094971 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.091120958 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.091130972 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.091154099 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.091161013 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.091186047 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.091190100 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.091217995 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.091226101 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.091259003 CET	49699	8082	192.168.2.3	20.104.209.69
Jan 8, 2023 16:12:04.210601091 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.210664034 CET	8082	49699	20.104.209.69	192.168.2.3
Jan 8, 2023 16:12:04.210747004 CET	8082	49699	20.104.209.69	192.168.2.3

HTTP Request Dependency Graph

- https:
  - 20.104.209.69:8082

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **4696**, Parent PID: **1260**

General

Target ID:	0

Start time:	16:11:59
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c sc create qFrdg binpath= "C:\Users\user\Desktop\8082-svc-x64.exe" >> C:\servicereg.log 2>&1
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Analysis Process: conhost.exe PID: **5368**, Parent PID: **4696**

General

Target ID:	1
Start time:	16:11:59
Start date:	08/01/2023
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: sc.exe PID: **5296**, Parent PID: **4696**

General

Target ID:	2
Start time:	16:11:59
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc create qFrdg binpath= "C:\Users\user\Desktop\8082-svc-x64.exe"
Imagebase:	0xef0000
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	EFB97A	WriteFile

Analysis Process: cmd.exe PID: **5280**, Parent PID: **1260**

General	
Target ID:	3
Start time:	16:12:00
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c sc start qFrdg >> C:\servicestart.log 2>&1
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File 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	BD194	CreateFileW

Analysis Process: conhost.exe PID: **5208**, Parent PID: **5280**

General	
Target ID:	4
Start time:	16:12:00
Start date:	08/01/2023
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: sc.exe PID: **588**, Parent PID: **5280**

General	
Target ID:	5
Start time:	16:12:00
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc start qFrdg
Imagebase:	0xef0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\servicestart.log	0	421	0d 0a 53 45 52 56 49 43 45 5f 4e 41 4d 45 3a 20 71 46 72 64 67 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 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: qFrdg TYPE : 10 WIN32_OWN_PROCESS STATE : 2 START_PENDING (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN) WIN32_EXIT_CODE : 0 (0x0) S	success or wait	1	EF5C54	WriteFile

Analysis Process: 8082-svc-x64.exe PID: **4044**, Parent PID: **580**

General

Target ID:	6
Start time:	16:12:01
Start date:	08/01/2023
Path:	C:\Users\user\Desktop\8082-svc-x64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\8082-svc-x64.exe
Imagebase:	0x400000
File size:	289280 bytes
MD5 hash:	89BE3BE20CA0DCE73C12A5A015BCB9A5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: CobaltStrike_Sleeve_BeaconLoader_VA_x64_o_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/BeaconLoader.VA.x64.o (VirtualAlloc) Versions 4.3 through at least 4.6, Source: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: Cobaltbaltstrike_Beacon_x64, Description: Detects CobaltStrike payloads, Source: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: CobaltStrike_MZ_Launcher, Description: Detects CobaltStrike MZ header ReflectiveLoader launcher, Source: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.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: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_4, Description: Yara detected CobaltStrike, Source: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000006.00000002.253882349.0000000000650000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\MSSE-7413-server	unknown	265731	success or wait	1	4018D8	ReadFile

Analysis Process: rundll32.exe PID: **3988**, Parent PID: **4044**

General

Target ID:	7
Start time:	16:12:02
Start date:	08/01/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\rundll32.exe
Imagebase:	0x7ff7a25b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.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: 00000007.00000002.772021320.00000270F7ECF000.00000004.00000001.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000007.00000003.258338449.00000270F7ECF000.00000004.00001000.00020000.00000000.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: 00000007.00000003.258338449.00000270F7ECF000.00000004.00001000.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000007.00000003.259556470.00000270F7ECF000.00000004.00001000.00020000.00000000.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: 00000007.00000003.259556470.00000270F7ECF000.00000004.00001000.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000007.00000003.258433014.00000270F7ECF000.00000004.00001000.00020000.00000000.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: 00000007.00000003.258433014.00000270F7ECF000.00000004.00001000.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: CobaltStrike_Sleeve_BeaconLoader_VA_x64_o_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/BeaconLoader.VA.x64.o (VirtualAlloc) Versions 4.3 through at least 4.6, Source: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: Cobaltbaltstrike_Beacon_x64, Description: Detects CobaltStrike payloads, Source: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: CobaltStrike_MZ_Launcher, Description: Detects CobaltStrike MZ header ReflectiveLoader launcher, Source: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.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: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_4, Description: Yara detected CobaltStrike, Source: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000007.00000003.253775962.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: unknown • Rule: CobaltStrike_Sleeve_BeaconLoader_VA_x64_o_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/BeaconLoader.VA.x64.o (VirtualAlloc) Versions 4.3 through at least 4.6, Source: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: gssincla@google.com • Rule: Cobaltbaltstrike_Beacon_x64, Description: Detects CobaltStrike payloads, Source: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: CobaltStrike_MZ_Launcher, Description: Detects CobaltStrike MZ header ReflectiveLoader launcher, Source: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.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: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_4, Description: Yara detected CobaltStrike, Source: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000007.00000000.253606501.00000270F7DF0000.00000020.00000400.00020000.00000000.sdmp, Author: unknown

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: svchost.exe PID: **2292**, Parent PID: **580**

General

Target ID:	8
Start time:	16:12:15
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:	0x7ff651c80000
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: **3112**, Parent PID: **580**

General

Target ID:	9
Start time:	16:12:15
Start date:	08/01/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
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	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

Analysis Process: svchost.exe PID: **5384**, Parent PID: **580**

General

Target ID:	10
Start time:	16:12:19
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:	0x7ff651c80000
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: **5320**, Parent PID: **580**

General

Target ID:	11
Start time:	16:12:20
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:	0x7ff651c80000
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: 5648, Parent PID: 580

General

Target ID:	12
Start time:	16:12:20
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:	0x7ff651c80000
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: 1844, Parent PID: 580

General

Target ID:	13
Start time:	16:12:20
Start date:	08/01/2023
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6904a0000
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: 5280, Parent PID: 580

General

Target ID:	14
Start time:	16:12:21
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:	0x7ff651c80000
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

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

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: **3548**, Parent PID: **580**

General

Target ID:	15
Start time:	16:12:21
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:	0x7ff651c80000
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: svchost.exe PID: **496**, Parent PID: **580**

General

Target ID:	16
Start time:	16:12:22
Start date:	08/01/2023

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff651c80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: **5628**, Parent PID: **3548**

General

Target ID:	17
Start time:	16:13:22
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:	0x7ff73e320000
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	9968	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 0d 00 0a 00	---	success or wait	1	7FF73E34BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10150	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 31 00 33 00 3a 00 32 00 33 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sun Jan 08 2023 16:13:23	success or wait	1	7FF73E34BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10408	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	7FF73E34BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10494	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	7FF73E34BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10514	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	7FF73E34BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10600	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 31 00 33 00 3a 00 32 00 33 00 0d 00 0a 00	MpCmdRun: End Time: Sun Jan 08 2023 16:13:23	success or wait	1	7FF73E34BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10700	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 0d 00 0a 00	--	success or wait	1	7FF73E34BC96	WriteFile

Analysis Process: conhost.exe PID: **5108**, Parent PID: **5628**

General

Target ID:	18
Start time:	16:13:22
Start date:	08/01/2023
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:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly