ID: 878635
Sample Name: 5q4psw.msi
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:58:31
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

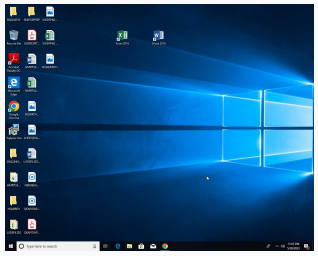
Windows Analysis Report

5q4psw.msi

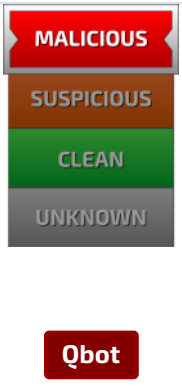
Overview

General Information

Sample Name:	5q4psw.msi
Analysis ID:	878635
MD5:	e35727b10193…
SHA1:	9ddafa77fc9fde..
SHA256:	696156d9a411…
Tags:	msi
Infos:	



Detection



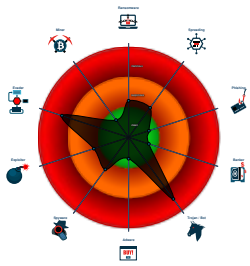
Qbot

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Qbot
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Sample uses string decryption to hid…
- Potentially malicious time measurem…
- Queries the volume information (nam…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 6716 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\5q4psw.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 5660 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - rundll32.exe (PID: 3676 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 3920 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - wermgr.exe (PID: 6000 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - wscript.exe (PID: 7012 cmdline: wscript.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\notify.vbs MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
QakBot, qbotQbot	QBot is a modular information stealer also known as Qakbot or Pinkslipbot. It has been active for years since 2007. It has historically been known as a banking Trojan, meaning that it steals financial data from infected systems, and a loader using C2 servers for payload targeting and download.	• GOLD CABIN	**http://** contagiodump.blogspot.com/2010/11/template.htmlhttp://www.secureworks.com/research/threat-profiles/gold-lagoonhttp://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf https://0xthreatintel.medium.com/reversing-qakbot-tlp-white-d1b8b37ad8e7https://asec.ahnlab.com/en/44662/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot

Malware Configuration

Threatname: Qbot

```
{
  "Bot id": "obama265",
  "Campaign": "1685436052",
  "Version": "404.1320",
  "C2 list": [
    "103.42.86.42:995",
    "174.4.89.3:443",
    "161.142.103.187:995",
    "78.160.146.127:443",
    "84.35.26.14:995",
    "12.172.173.82:20",
    "70.28.50.223:2078",
    "124.149.143.189:2222",
    "70.160.67.203:443",
    "186.64.67.30:443",
    "103.123.223.133:443",
    "94.207.104.225:443",
    "89.114.140.100:443",
    "213.64.33.61:2222",
    "86.176.144.234:2222",
    "72.134.124.16:443",
    "47.34.30.133:443",
    "109.50.149.241:2222",
    "85.104.105.67:443",
    "81.111.108.123:443",
    "86.173.2.12:2222",
    "188.28.19.84:443",
    "41.228.224.161:995",
    "12.172.173.82:50001",
    "178.175.187.254:443",
    "65.95.141.84:2222",
    "205.237.67.69:995",
    "83.110.223.61:443",
    "193.253.100.236:2222",
    "27.0.48.233:443",
    "102.159.188.125:443",
    "71.38.155.217:443",
    "58.186.75.42:443",
    "76.178.148.107:2222",
    "70.28.50.223:2087",
    "114.143.176.236:443",
    "51.14.29.227:2222",
    "59.28.84.65:443",
    "173.88.135.179:443",
    "103.144.201.56:2078",
    "96.87.28.170:2222",
    "105.184.103.97:995",
    "176.142.207.63:443",
    "151.62.238.176:443",
    "12.172.173.82:32101",
    "122.186.210.254:443",
    "82.125.44.236:2222",
    "84.108.200.161:443",
    "76.16.49.134:443",
    "70.28.50.223:32100",
    "12.172.173.82:465",
    "76.170.252.153:995",
    "184.182.66.109:443",
    "78.92.133.215:443",
    "50.68.204.71:993",
    "186.75.95.6:443",
    "113.11.92.30:443",
    "70.28.50.223:3389",
    "98.145.23.67:443",
    "85.57.212.13:3389",
    "50.68.186.195:443",
    "47.205.25.170:443",
    "12.172.173.82:993",
    "12.172.173.82:22",
    "69.242.31.249:443",
    "81.101.185.146:443",
    "79.168.224.165:2222",
    "75.143.236.149:443",
    "14.192.241.76:995",
    "86.195.14.72:2222",
    "81.229.117.95:2222",
    "220.240.164.182:443",
    "73.29.92.128:443",
    "12.172.173.82:21",
    "96.56.197.26:2222",
    "75.109.111.89:443",
    "76.86.31.59:443",
    "201.244.108.183:995",
    "68.203.69.96:443",
    "124.122.47.148:443",
    "122.184.143.86:443",
    "92.186.69.229:2222",
    "70.28.50.223:2083",
    "89.129.109.27:2222",
    "147.147.30.126:2222",
```

```
    "125.99.76.102:443",
    "88.126.94.4:50000",
    "151.65.167.77:443",
    "86.132.236.117:443",
    "92.154.17.149:2222",
    "223.166.13.95:995",
    "89.36.206.69:995",
    "96.56.197.26:2083",
    "78.18.105.11:443",
    "82.127.153.75:2222",
    "90.78.147.141:2222",
    "82.131.141.209:443",
    "183.87.163.165:443",
    "92.9.45.20:2222",
    "80.6.50.34:443",
    "80.12.88.148:2222",
    "69.133.162.35:443",
    "172.115.17.50:443",
    "95.45.50.93:2222",
    "12.172.173.82:2087",
    "103.140.174.20:2222",
    "24.198.114.130:995",
    "50.68.204.71:443",
    "69.119.123.159:2222",
    "64.121.161.102:443",
    "2.82.8.80:443",
    "184.181.75.148:443",
    "70.112.206.5:443",
    "198.2.51.242:993",
    "2.36.64.159:2078",
    "79.77.142.22:2222",
    "84.215.202.8:443",
    "147.219.4.194:443",
    "116.74.164.81:443",
    "70.28.50.223:2078"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.381770135.000000000360A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000004.00000002.381884570.0000000005230000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
decrypted.memstr	JoeSecurity_Qbot	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.4fb0000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
4.2.rundll32.exe.4fb0000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.rundll32.exe.3620a00.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xdf71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9b97:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
4.2.rundll32.exe.3620a00.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.rundll32.exe.3620a00.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3

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

Found malware configuration

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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

Anti Debugging

Potentially malicious time measurement code found

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Qbot

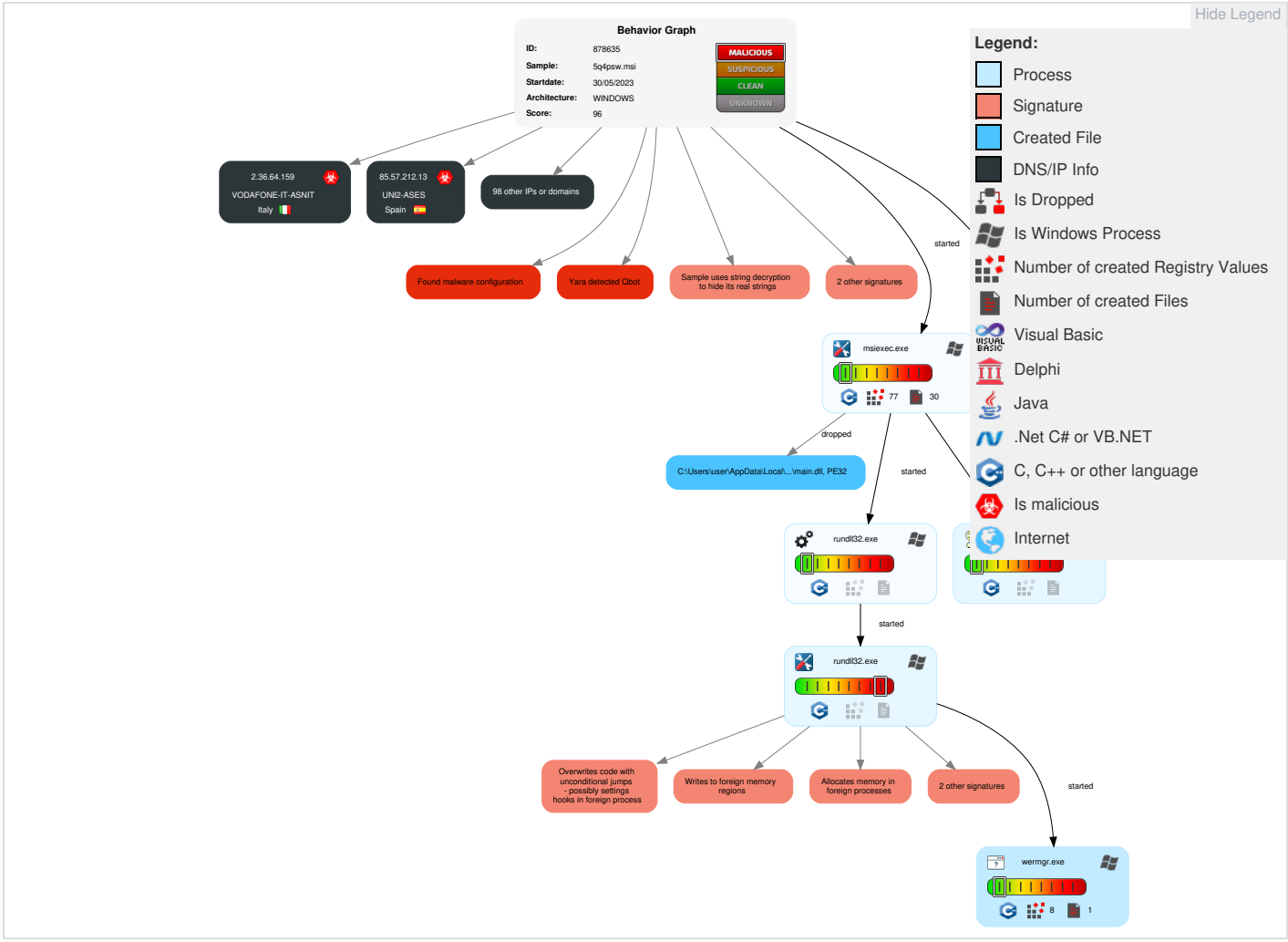
Remote Access Functionality

Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 1 Scripting	1 DLL Side-Loading	3 1 1 Process Injection	1 1 Masquerading	1 Credential API Hooking	2 System Time Discovery	1 Replication Through Removable Media	1 Credential API Hooking	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 2 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 Peripheral Device Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Scripting	Cached Domain Credentials	2 4 System Information 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 Obfuscated Files or Information	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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	Network Service Scanning	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)	1 DLL Side-Loading	/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 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

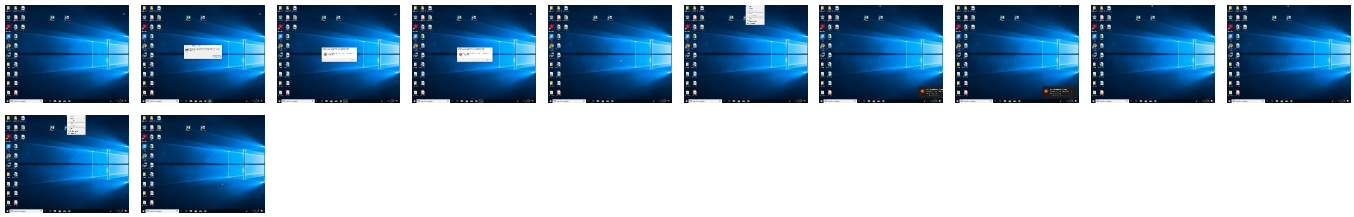
Behavior Graph



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
5q4psw.msi	5%	ReversingLabs		
5q4psw.msi	5%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	5%	ReversingLabs		
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	4%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

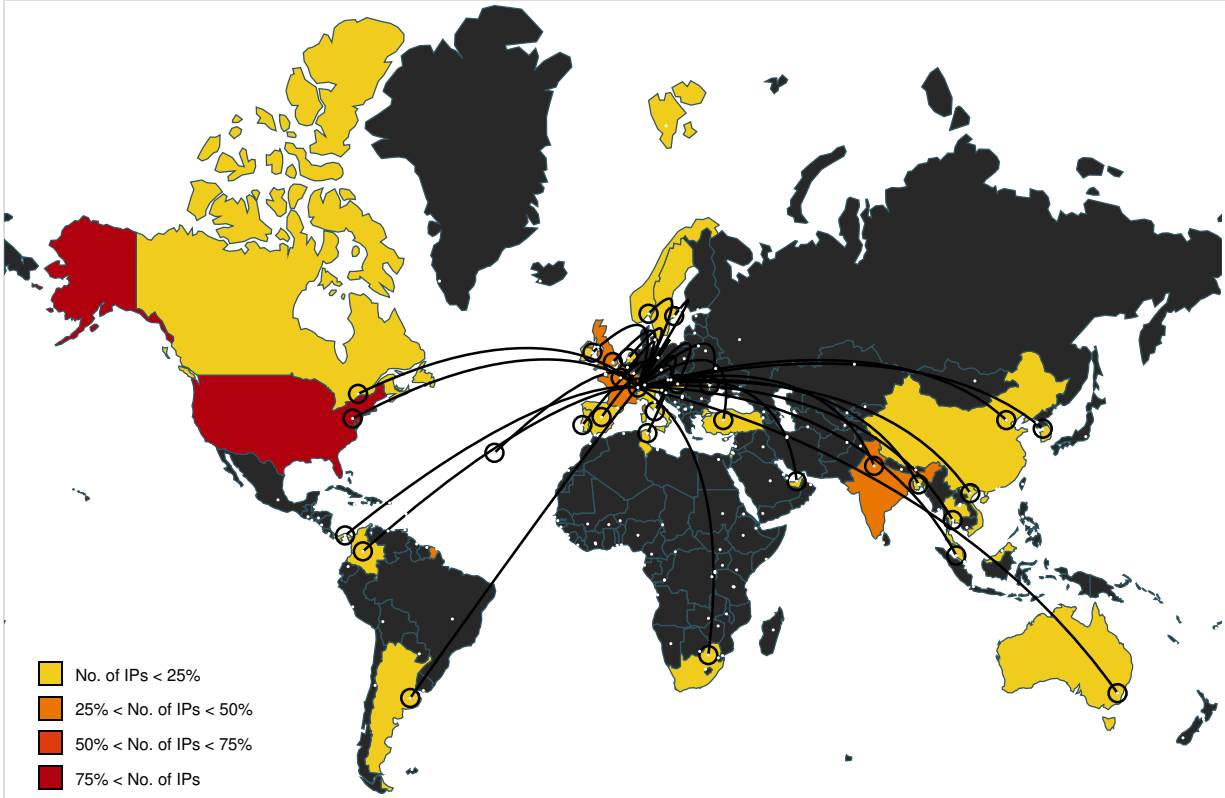
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://streams.videolan.org/upload/	rundll32.exe, rundll32.exe, 00000004.00000002.382108966.00000000100AB000.00000002.00000001.01000000.00000003.sdmp, main.dll.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.82.8.80	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
70.160.67.203	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
75.143.236.149	unknown	United States		20115	CHARTER-20115US	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
86.195.14.72	unknown	France		3215	FranceTelecom-OrangeFR	true
84.215.202.8	unknown	Norway		41164	GET-NOGETNorwayNO	true
184.182.66.109	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
105.184.103.97	unknown	South Africa		37457	Telkom-InternetZA	true
92.186.69.229	unknown	France		12479	UNI2-ASES	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
14.192.241.76	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
173.88.135.179	unknown	United States		10796	TWC-10796-MIDWESTUS	true
84.108.200.161	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	true
47.34.30.133	unknown	United States		20115	CHARTER-20115US	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true
124.149.143.189	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
84.35.26.14	unknown	Netherlands		21221	INFOPACT-ASTheNetherlandsNL	true
73.29.92.128	unknown	United States		7922	COMCAST-7922US	true
68.203.69.96	unknown	United States		11427	TWC-11427-TEXASUS	true
82.131.141.209	unknown	Hungary		20845	DIGICABLEHU	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
178.175.187.254	unknown	Moldova Republic of		43289	TRABIAMD	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
186.64.67.30	unknown	Argentina		27953	NODOSUDSAAR	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
86.176.144.234	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
59.28.84.65	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
76.86.31.59	unknown	United States		20001	TWC-20001-PACWESTUS	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
96.87.28.170	unknown	United States		7922	COMCAST-7922US	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
78.92.133.215	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
88.126.94.4	unknown	France		12322	PROXADFR	true
51.14.29.227	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
85.57.212.13	unknown	Spain		12479	UNI2-ASES	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
80.12.88.148	unknown	France		3215	FranceTelecom-OrangeFR	true
81.111.108.123	unknown	United Kingdom		5089	NTLGB	true
69.133.162.35	unknown	United States		11426	TWC-11426-CAROLINASUS	true
86.132.236.117	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
151.62.238.176	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
70.112.206.5	unknown	United States		11427	TWC-11427-TEXASUS	true
41.228.224.161	unknown	Tunisia		37693	TUNISIANATN	true
205.237.67.69	unknown	Canada		11290	CC-3272CA	true
102.159.188.125	unknown	Tunisia		37705	TOPNETTN	true
151.65.167.77	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
76.178.148.107	unknown	United States		10838	OCEANIC-INTERNET-RRUS	true
89.36.206.69	unknown	Italy		48544	TECNOADSL-ASIT	true
69.242.31.249	unknown	United States		7922	COMCAST-7922US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.104.105.67	unknown	Turkey		9121	TTNETTR	true
94.207.104.225	unknown	United Arab Emirates		15802	DU-AS1AE	true
193.253.100.236	unknown	France		3215	FranceTelecom-OrangeFR	true
76.16.49.134	unknown	United States		7922	COMCAST-7922US	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
78.18.105.11	unknown	Ireland		2110	AS-BTIREBTIrelandwaspreviouslyknownasEsatNetEUnet	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
103.144.201.56	unknown	unknown		139762	MSSOLUTION-AS-APSolutionBD	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
98.145.23.67	unknown	United States		20001	TWC-20001-PACWESTUS	true
82.125.44.236	unknown	France		3215	FranceTelecom-OrangeFR	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
89.129.109.27	unknown	Spain		12479	UNI2-ASES	true
122.186.210.254	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
90.78.147.141	unknown	France		3215	FranceTelecom-OrangeFR	true
122.184.143.86	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
213.64.33.61	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
86.173.2.12	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
78.160.146.127	unknown	Turkey		9121	TTNETTR	true
58.186.75.42	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
50.68.204.71	unknown	Canada		6327	SHAWCA	true
71.38.155.217	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
220.240.164.182	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
24.198.114.130	unknown	United States		11351	TWC-11351-NORTHEASTUS	true
2.36.64.159	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
198.2.51.242	unknown	United States		20001	TWC-20001-PACWESTUS	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
109.50.149.241	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
69.119.123.159	unknown	United States		6128	CABLE-NET-1US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.115.17.50	unknown	United States		20001	TWC-20001-PACWESTUS	true
147.219.4.194	unknown	United States		1498	DNIC-ASBLK-01498-01499US	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878635
Start date and time:	2023-05-30 22:58:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsofficecookbook.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:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	10
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
Sample file name:	5q4psw.msi
Detection:	MAL
Classification:	mal96.troj.evad.winMSI@10/21@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 4.6% (good quality ratio 2%) • Quality average: 17.8% • Quality standard deviation: 26.1%
HCA Information:	• Successful, ratio: 67% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .msi • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:59:40	API Interceptor	9x Sleep call for process: wermgr.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:\Config.Msi\55f8bb.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	8918
Entropy (8bit):	5.573518641830586
Encrypted:	false
SSDEEP:	96:FrM2eKeCyGS2U/yyPw9CsvRqnU/yyPw9C6jSnHU/vRq1HVPYf8NaoKcw5wDPavCT:F5e9/yOwg+/yOwgio5tUVpO
MD5:	EE90792188E08D70C180F92AB318B1CA
SHA1:	564EA5BF0155320A9635B895DF5AF6298DC2DFFF
SHA-256:	1A74745599EA2B3C75E34490D7682EF6E1EAEF6AD62361422CA7A2CF3A8C7E43
SHA-512:	97A255A89E56C2311EB61801563030243E3E9BFE5B9BF66373C950468B012F47B63FEDE35A8BD18D99BEF1D7A2844EE0614D0C6A82E39FCF51D7526E649BC57
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@p..V.@.....@.....@.....@.....@.....@.....&.{2DB09FCD-7D8E-4C24-BF5D-FB5BD25D67B7}'.Adobe Acrobat PDF Browser Plugin 4.8.25..5q4psw.ms i.@.....@.....@.....@.....@.....@.....&.{D557C495-7A3E-4038-8369-B6EDCD5EFABE}.....@.....@.....@.....@.....@.....@.....@.....@.....@....'.Adobe Acrobat PDF Browser Plugin 4.8.25.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{82B5B2FD-2237-42AB-9F03-B3B9EAB30000}&.{2DB09FCD-7D8E-4C24-BF5D-FB5BD25D67B7}.@.....InstallFiles..Copying new files&.File: [1], Directory: [9], Size: [6]..:.C :\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\....B.C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll....D.C:\Users\user\App Data\Local\AdobeAcrobatPDFBrowserPlugin\notify.vbs....WriteRegistryValues..Writing system registry values..Key: [1], Name: [2], Value: [3]$..@....%.Software\Ado beAcrobatPDFBrowserPlugin...@....(.&...AdobeAcrobatPDFBro

C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	952832
Entropy (8bit):	6.765764209638377
Encrypted:	false
SSDEEP:	24576:UkgLxg2eMP8EN8Vo7zgDQ9uo4iZSBi/u3wXqx9jKVM5qx0YJ:x/jDQMo49wpq
MD5:	0C8E5B12B177A199008B2282C7506FFF
SHA1:	0DFEE8BAE7073512F8BFDABAF0C0B7C882B3864E
SHA-256:	9A407A2F0BA3C0E3BA3CFA2FFD6472DB3BC572B8EF08F1FBA7139CBD36CC8DCA
SHA-512:	6464EC42CCCB85E7C067AD9F7C8B804D064A6974E8184BC5134436FAD004BF87630869C107BB91F87BDC59F7938A8A157F59A436CE0265C070DB32A54C4541B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 5% • Antivirus: Virustotal, Detection: 4%, Browse
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...m..d.....#...8..... ....@... .....hC.....<..... ...?.....$J.....text...4.....`.0`.data.....@.0..rda ta..|.....@.0@.bss....D....p.....>.....0..edata..hC.....D...>.....@.0@.idata..<.....@.0..CRT....0.....@.0..tls..... .....@.0..rsrc...b.....@.0..reloc...?.....@...J.....@.0B..... .....

C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\notify.vbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	132
Entropy (8bit):	4.599233980549996
Encrypted:	false
SSDEEP:	3:LwBxFkvH4dGmMKLVKRLGPz4VAFkvH4dGmMKLVKRLGH:cHFkvYdlZKRLi7FkvYdlZKRL4
MD5:	0D4C9F15CE74465C59AE36A27F98C817
SHA1:	9CCE8EEFA4D3D9C5E161C5DBB860CFE1489C6B1A
SHA-256:	D24E3399060B51F3A1C9D41A67DE2601888A35C99DA8DB70070D757BB3F1913A
SHA-512:	9BED0EAFC2CF2A2360850CA1070FFB04AC14F04C78379485998A93F45012B5C11CC7F6F68129F65B8B5F90437CB965908C6A1BB9D83A56B068D6BDE1D5FDADF
Malicious:	false
Preview:	MsgBox "Adobe Acrobat PDF Browser Plugin installation error 0x00000328", 16, "Adobe Acrobat PDF Browser Plugin installation error"..

C:\Windows\Installer\55f8ba.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Adobe Acrobat PDF Browser Plugin 4.8.25, Author: Adobe Inc., Keywords: Installer, Comments: Adobe Acrobat PDF Browser Plugin, Template: Intel;1033, Revision Number: {D557C495-7A3E-4038-8369-B6EDCD5EFABE}, Create Time/Date: Tue May 30 14:26:08 2023, Last Saved Time/Date: Tue May 30 14:26:08 2023, Number of Pages: 200, Number of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Category:	dropped
Size (bytes):	507904
Entropy (8bit):	7.919619627017417
Encrypted:	false
SSDEEP:	12288:wn+NgINNEcfjVRMigNFoILI8KviLjvhAol71Q:wnX9gjVRMDqH8fL154
MD5:	E35727B10193FE55DF216A1F9D166997
SHA1:	9DDAFA77FC9FDEA0085E41AA0F3A1EE0D15D9C8A
SHA-256:	696156D9A4117CBA652B18B012DB376FDDFBD7DB8B26A638C760D61B98D3590D
SHA-512:	2BBA74B0B7F5EE8509310030BB45DEF13B87394E55EDF8D0E51595D6CC669F4B2C7497D95331C09C9F7B453F3C9ACDEB03E41CD5E5DC14F9ECB9DD9F79D7AD8D
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\55f8bc.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Adobe Acrobat PDF Browser Plugin 4.8.25, Author: Adobe Inc., Keywords: Installer, Comments: Adobe Acrobat PDF Browser Plugin, Template: Intel;1033, Revision Number: {D557C495-7A3E-4038-8369-B6EDCD5EFABE}, Create Time/Date: Tue May 30 14:26:08 2023, Last Saved Time/Date: Tue May 30 14:26:08 2023, Number of Pages: 200, Number of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Category:	dropped
Size (bytes):	507904
Entropy (8bit):	7.919619627017417
Encrypted:	false
SSDEEP:	12288:wn+NgINNEcfjVRMigNFoILI8KviLjvhAol71Q:wnX9gjVRMDqH8fL154
MD5:	E35727B10193FE55DF216A1F9D166997
SHA1:	9DDAFA77FC9FDEA0085E41AA0F3A1EE0D15D9C8A
SHA-256:	696156D9A4117CBA652B18B012DB376FDDFBD7DB8B26A638C760D61B98D3590D
SHA-512:	2BBA74B0B7F5EE8509310030BB45DEF13B87394E55EDF8D0E51595D6CC669F4B2C7497D95331C09C9F7B453F3C9ACDEB03E41CD5E5DC14F9ECB9DD9F79D7AD8D
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSIFB1B.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	5.597289542209639
Encrypted:	false
SSDEEP:	48:UWozIAJwCP3RDufgjYjRBoD8SY1eU/Vn0VaEVltgI4tK:UrMiHYjrAueywaEPNT
MD5:	D3DEA972DEEE8C5C7555BD734F9CE893
SHA1:	7DFE0F36C98DED75BED0AED621F42017EF914405
SHA-256:	50FCA99410D3EB92701142C205A548AF9510A4828E5A199976F6C69D8C7C2246
SHA-512:	C7C515090202A477F4E9204DF48C38C39CD0F0F270C1C462875B956B9697DF42DFAD570D22F47DD6CBD6A86E2AC8BC0A9198618A980306DDD653B6C50D1396
Malicious:	false
Preview:	...@IXOS.@.....@p..V.@.....@.....@.....@.....@.....@.....&.{2DB09FCD-7D8E-4C24-BF5D-FB5BD25D67B7}'.Adobe Acrobat PDF Browser Plugin 4.8.25..5q4psw.ms i.@.....@.....@.....@.....@.....&.{D557C495-7A3E-4038-8369-B6EDCD5EFABE}.....@.....@.....@.....@.....@.....@.....@.....@.....@....'.Adobe Acrobat PDF Browser Plugin 4.8.25.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.. ...@.....@.....@.]....&.{82B5B2FD-2237-42AB-9F03-B3B9EAB30000}F.01:\Software\AdobeAcrobatPDFBrowserPlugin\AdobeAcrobatPDFBrowserPlugin.@.....@.....@ .....@.....InstallFiles..Copying new files&.File: [1], Directory: [9], Size: [6]...@.....@.....@.....:.C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\..). 1\xssanpen|AdobeAcrobatPDFBrowserPlugin\.....Please insert the disk: ..media3.cab.@.....@.....C:\Windows\Installer\55f8ba.msi.....@.....main.dll..dll_main..main .dll.@.....@.....@.....@...

C:\Windows\Installer\SourceHash{2DB09FCD-7D8E-4C24-BF5D-FB5BD25D67B7}	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1632735510729422
Encrypted:	false
SSDEEP:	12:JSbX72FjSAGiLIlHVRpth/77777777777777777777777vDHFSiOdbEpSl0i8Q:JoQl5pidyF
MD5:	89D586E6AD6BEA01405949AF0BCA8A3A
SHA1:	2A73885282EB60DB9282FDDEFFB230D6AE3AE58B
SHA-256:	2FD787A10D63E9C2FEFBAFA9D4C424AC6893324A86D7EBE6C70D76BB6FAE39FD
SHA-512:	F38C1415A526A95CDB97077F59E0663CDAFA161B9EDFAB307893FF3D9A6F42E728248DCB242B54D54F4403421413A84A41D72FC96E4968A77ACE9D341C915C9
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5058400020774245
Encrypted:	false
SSDEEP:	48:q8PhfuRc06WXJ8FT57XgKuLMS5khp/rD6uLMSI818lP0:1hf1fFTVhvO
MD5:	6541081204CC56B31158430D26D58503
SHA1:	F3C2C50652559EC9AD81ACF9EE9A7B0492F784C3
SHA-256:	CDDCDF00A887B6E25DE72F11DADCBF93A0E85D1470F13B6569E442F736C89AE6
SHA-512:	E383B49FF2A65CC8EE0183DC97EF9B0EBEEB42E48EEF563A73329288B6A294941372CAC8F1EB67950F9EA0FC021BF0BA0988D9E4ACF952B0A9D34136CC3D4A F5
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators

Category:	dropped
Size (bytes):	192827
Entropy (8bit):	5.392015123446331
Encrypted:	false
SSDEEP:	3072:iHHJCoX5CNWFHjkzRl1pqf5JjzH6wbxygaK8Nkv6kF8Kwu8K8uBD556GIlZZ6bF7:i0LVlAp
MD5:	15A5D3FA6B4EFC956BFA3F1D4A6EA388
SHA1:	C077B611A721916F881B285BC496EC9B832A84A7
SHA-256:	15C927A1CB8FE141AE5869A43BEE0F915ACE9782344CCA811352F6F6C85FD56B
SHA-512:	8F055DE0656521E54BCBADE507536FE2805BABCF9DA23038CAC1818416BB2AA0105761D51F9FC6E26F77F3D6823D1B21B9CB1BA4343AAA453C5299402A00AA9 8
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 10:13:25.847 [3928]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.Hosting, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.863 [3928]: ngen returning 0x00000000..07/23/2020 10:13:25.925 [1900]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.ServerDocument, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.925 [1900]: ngen returning 0x00000000..07/23/2020 10:13:25.972 [4436]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.v4.0.Framework, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /N

C:\Windows\Temp\~DF092DC5D1FEAA268C.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2099972641536612
Encrypted:	false
SSDEEP:	48:rsHugPveFXJxT5vXgKuLMS5khp/rD6uLMSI818lP0:IHAJTZhvO
MD5:	FD26F1A8E0428DC71ADD67C7258E7FC4
SHA1:	09021EC33DE22A721F2DA959584828D79E989251
SHA-256:	3D7E84CDEF142BBCF468F9EAA5C877F8B53C4F0EFFF84DA7D45134830EA3CAC7
SHA-512:	D2F007B25B05D4F658004CD15CA6EE655CEB8497C6B183AA355AEFE5EEF5DF1CE65DA12C6631C419F8CBC84A6D27ED951FFCD3C47851CC142CC897DAF052 E05
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF3AFD14CAA7749B80.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2099972641536612
Encrypted:	false
SSDEEP:	48:rsHugPveFXJxT5vXgKuLMS5khp/rD6uLMSI818lP0:IHAJTZhvO
MD5:	FD26F1A8E0428DC71ADD67C7258E7FC4
SHA1:	09021EC33DE22A721F2DA959584828D79E989251
SHA-256:	3D7E84CDEF142BBCF468F9EAA5C877F8B53C4F0EFFF84DA7D45134830EA3CAC7
SHA-512:	D2F007B25B05D4F658004CD15CA6EE655CEB8497C6B183AA355AEFE5EEF5DF1CE65DA12C6631C419F8CBC84A6D27ED951FFCD3C47851CC142CC897DAF052 E05
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF3F77F918320563FF.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF4A6271EF11B37377.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.06981105571250576
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOSlgOda8971N5QVky6lS:2F0i8n0itFzDHFSiOdbFS
MD5:	5958014AA25C5536AC922FB0F2586B9F
SHA1:	AE9F32F875238BDDEA22C343217DF64FB74AFE59
SHA-256:	D4E0FBF5B4E51B6A1076DFBE9B346D390714A0F796BC73C9D2CB187793961966
SHA-512:	DF3C3E2E61AB5EAB0C4A5CCEC40A07F9E3491CE7C0D6C4A74D476ADD9179A6494963789898DCD7E5741BCD9437B01E4D333F08729EAFDB37220BEB3647C0E73A
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF5555397D86C72808.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2099972641536612
Encrypted:	false
SSDEEP:	48:rsHugPveFXJxT5vXgKuLMS5khp/rD6uLMSI818lP0:IHAJTZhvO
MD5:	FD26F1A8E0428DC71ADD67C7258E7FC4
SHA1:	09021EC33DE22A721F2DA959584828D79E989251
SHA-256:	3D7E84CDEF142BBCF468F9EAA5C877F8B53C4F0EFFF84DA7D45134830EA3CAC7
SHA-512:	D2F007B25B05D4F658004CD15CA6EE655CEB8497C6B183AA355AEFE5EEF5DF1CE65DA12C6631C419F8CBC84A6D27ED951FFCD3C47851CC142CC897DAF052E05
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFA48F4C3EB3ED2F6F.TMP

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

Malicious:	false
Preview:	....

C:\Windows\Temp\~DFB2E09CA8BE461258.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFB404815109B1126A.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5058400020774245
Encrypted:	false
SSDEEP:	48:q8PhfuRc06WXJ8FT57XgKuLMS5khp/rD6uLMSI818lP0:1hf1fFTVhvO
MD5:	6541081204CC56B31158430D26D58503
SHA1:	F3C2C50652559EC9AD81ACF9EE9A7B0492F784C3
SHA-256:	CDDCDF00A887B6E25DE72F11DADCBF93A0E85D1470F13B6569E442F736C89AE6
SHA-512:	E383B49FF2A65CC8EE0183DC97EF9B0EBEEB42E48EEF563A73329288B6A294941372CAC8F1EB67950F9EA0FC021BF0BA0988D9E4ACF952B0A9D34136CC3D4A F5
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFC45B0184A39B8DFE.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFCBDFB5D5B5D930C1.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped

Size (bytes):	69632
Entropy (8bit):	0.12081938981088994
Encrypted:	false
SSDEEP:	24:IUM70R818lOdWmOLqrb9ipVIdWmOLqrb9ipV7VO3wGtpJlrkg0+vB9J:D7R818lEuLMSouLMS5khp/r0gB
MD5:	7CE53BC4D5E97E3826DA403AD75C1ABF
SHA1:	337C7F389ADD4D4F3BB48CD0CC0071148E39685F
SHA-256:	B938E86FAE42605D29F33FECAB09EA5C72FC239AF372E93EC4F3E2F862061970
SHA-512:	B88CEF3E105D38543BABEB2AAF29A4BDF22932CA17B6E5D4F7532604C24E64378958932A7126CF9186159B327044852051EDA27854A4F090EBFF73B2E761BB7F
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFD8BC86747873A537.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5058400020774245
Encrypted:	false
SSDEEP:	48:q8PhfuRc06WXJ8FT57XgKuLMS5khp/rD6uLMSI818lP0:1hf1fFTVhvO
MD5:	6541081204CC56B31158430D26D58503
SHA1:	F3C2C50652559EC9AD81ACF9EE9A7B0492F784C3
SHA-256:	CDDCDF00A887B6E25DE72F11DADCBF93A0E85D1470F13B6569E442F736C89AE6
SHA-512:	E383B49FF2A65CC8EE0183DC97EF9B0EBEEB42E48EEF563A73329288B6A294941372CAC8F1EB67950F9EA0FC021BF0BA0988D9E4ACF952B0A9D34136CC3D4A F5
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFFD09074CA4B5BB91.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Adobe Acrobat PDF Browser Plugin 4.8.25, Author: Adobe Inc., Keywords: Installer, Comments: Adobe Acrobat PDF Browser Plugin, Template: Intel;1033, Revision Number: {D557C 495-7A3E-4038-8369-B6EDCD5EFABE}, Create Time/Date: Tue May 30 14:26:08 2023, Last Saved Time/Date: Tue May 30 14:26:08 2023, Number of Pages: 200, Nu mber of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Entropy (8bit):	7.919619627017417
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	5q4psw.msi

File size:	507904
MD5:	e35727b10193fe55df216a1f9d166997
SHA1:	9ddafa77fc9fdea0085e41aa0f3a1ee0d15d9c8a
SHA256:	696156d9a4117cba652b18b012db376fddfbd7db8b26a638c760d61b98d3590d
SHA512:	2bba74b0b7f5ee8509310030bb45def13b87394e55edf8d0e51595d6cc669f4b2c7497d95331c09c9f7b453f3c9acdeb03e41cd5e5dc14f9ecb9dd9f79d7ad8d
SSDEEP:	12288:wn+NgINNEcfjVRMigNFoILI8KviLjvhAol71Q:wnX9gjVRMDqH8fL154
TLSH:	DDB423597606A371C4C82A72A63F77CAB6B17CA547074833C33FB2DE0D3657829267A1
File Content Preview:	.....>.....

File Icon

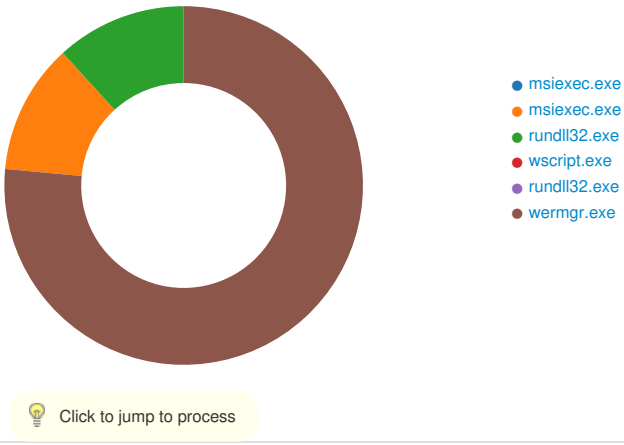
Icon Hash:	2d2e3797b32b2b99

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 6716, Parent PID: 3452

General

Target ID:	0
Start time:	22:59:29
Start date:	30/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\5q4psw.msi"
Imagebase:	0x7ff7baeb0000
File size:	66048 bytes

MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **5660**, Parent PID: **580**

General

Target ID:	1
Start time:	22:59:30
Start date:	30/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff7baeb0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
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 Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	192733	94	30 35 2f 33 30 2f 32 30 32 33 20 32 32 3a 35 39 3a 33 30 2e 38 32 34 20 5b 35 36 36 30 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	05/30/2023 22:59:30.824 [5660]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFC0B09BEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFC0B09BBC6	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **3676**, Parent PID: **5660**

General

Target ID:	2
Start time:	22:59:31
Start date:	30/05/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next
Imagebase:	0x7ff684e90000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	64	success or wait	1	7FF684E92FA7	ReadFile
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	264	success or wait	1	7FF684E92FEA	ReadFile

Analysis Process: wscript.exe PID: **7012**, Parent PID: **5660**

General

Target ID:	3
Start time:	22:59:31
Start date:	30/05/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	wscript.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\notify.vbs
Imagebase:	0x7ff7f07d0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **3920**, Parent PID: **3676**

General

Target ID:	4
Start time:	22:59:31
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next
Imagebase:	0x12e0000
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_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.381770135.000000000360A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.381884570.0000000005230000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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: wermgr.exe PID: **6000**, Parent PID: **3920**

General

Target ID:	5
Start time:	22:59:34
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x300000
File size:	191904 bytes
MD5 hash:	CCF15E662ED5CE77B5FF1A7AAE305233
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Pyqjqkupcd	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	32C2CEB	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	952832	success or wait	2	32CE746	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	success or wait	1	32CAC70	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	32351a59	binary	5E A6 CC 8C 41 DC 80 B2 37 68 4F 28 C2 86 0C 22 3F F0 1E 85 15 79 25 C2 26 80 67 54 26 CE 3C CA 88 EE 9C 56 42 67 18 0D 19 16 D3 7A 86 94 A2 D4 DE DC 53 EB 38 B8 88 BA 0F 56 FD 0B 01 5E 9E E4 69 81 3E 52 1C BE 5D 34 E9 50 19 57 8A 51 CD B6 F2 9E F4 56 80 07 3A CD 11 E1 22	success or wait	1	32CB195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	7aaca17	binary	33 84 6F 4B F1 C2 DE 9B 49 AA 42 D5 40 44 BE 16 48 D4 38 B9 07 5E 61 BE 67 A6 D6 E1 ED 1B 56 10 00 B4 D4 86 BF AF 22 91 0A 66 33 63 6A 1C 6E 12 EF AB 90 99 D3 B7 C9 A2 44 52 F5 29 39 1C 7F AA 63 22 28 74 50 91 5C EC B3 67 69 20 E0 20 C9 FA 89 BD 30 11 4F EE 5C 9C C9 E7 D8 A4 42 58 9B 9A C6 AC C8 AE 67 AE C6 AA 97 AB E9 E3 70 17 8E 7C 73 75 5F 92 E6 23 9F 77 EC B1 44 E6 A8 D5 F8 78 AB 17 B0 4C 24 89 85 50 45 2B 28 7E 80 6B CB 14 DC 14 82 8E 74 2C D9 D9	success or wait	1	32CB195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	5ebea6b	binary	E5 5C D0 A5 4B DF 20 15 C4 2A 8B 7F 07 0A 7D E4 0B A3 57 72 77 D9 69 29 86 F9 D5 F4 EF AF 8A 14 ED D9 F1 6E 59 8B E6 5F 47 9F 02	success or wait	1	32CB195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	bd578d0e	binary	0E CB A7 D4 7E 30 67 20 AC DE 66 0A F4 40 D5 D4 5E 10 CC 01 14 CC EF 9D 80 EB 99 59 A9 4C 62 E1 C7 00 B7 41 A0 D7 9C 9F F3 D6 B7 15 AA C4 E9 FE 5C CC 82 D1 83	success or wait	1	32CB195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	c05fc284	binary	F8 81 62 F4 91 56 1E 71 70 DC 2E A4 CF 5D E1 B6 9C 09 C6 B4 E1 28 FC	success or wait	1	32CB195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	78e3a5e1	binary	03 AA 48 F5 A6 16 EE 7D 86 4D 47 BB AF 1A DC 54 A4 04 0F B4 92 2D 91 85 9E 90 62 6E 0A C6 44 66 7F CE 76 7D	success or wait	1	32CB195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	bf16ad72	binary	C4 6D 6B ED C1 A3 91 3A 92 F5 B2 68 E0 64 B0 46 68 2A 4B 40 7E BE A3 90 1C F4 F1 29 EB 52 D4 FF 63 28 0D 72 8E EE 2E	success or wait	1	32CB195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	4d7c75af	binary	77 24 C7 30 BF C3 F2 69 F5 EC 21 15 24 28 C7 A3 07 42 DC 42 46 CE D7 69 66 3E 5A 30 32 CF DF 4B 2E E5 92 B7 FE 70 60 0F A3 8C 12 A2 BE 11 41 68 2D 73 83 C5 13 1E 75 E3 21 F1 17 65 3A 19 CF 68 48 BA 72 06 D4 18 76 92 9E D2 31 48 FC 0D 45 99 76 54 1A 21 1B B3 DF 8F 51 AA 7B 84 EF A3 58 ED 20 A9 DC CB 08 23 22 58 04 CC AF 7B 04 21 97 2A	success or wait	1	32CB195	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	32351a59	binary	5E A6 CC 8C 41 DC 80 B2 37 68 4F 28 C2 86 0C 22 3F F0 1E 85 15 79 25 C2 26 80 67 54 26 CE 3C CA 88 EE 9C 56 42 67 18 0D 19 16 D3 7A 86 94 A2 D4 DE DC 53 EB 38 B8 88 BA 0F 56 FD 0B 01 5E 9E E4 69 81 3E 52 1C BE 5D 34 E9 50 19 57 8A 51 CD B6 F2 9E F4 56 80 07 3A CD 11 E1 22	5E A6 D7 8C 41 DC B1 3F 32 A6 52 F9 34 95 AB 68 2F ED BF 41 A7 4E 14 BF 4F E4 E8 EC 6E 14 CA 2B 92 78 BC 90 F8 CD BB D2 3D A8 90 18 C6 C4 0D E6 7D F9 76 2D ED C6 3A 59 E0 9B 84 B1 95 8C 8E 3F FE D4 1E C9 97 33 8C A1 09 38 11 2D 5A B7 1A 73 94 12 A7 18 50 9C B3 61 13 3B E2 B5 6B 19 0E 5F 7B 52 51 DD 1B FA 60 EB 23 1B EB 06 F8 D4 BE 99 0F FB F6 5B	success or wait	1	32CB195	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Onhybhcunyojm	32351a59	binary	5E A6 D7 8C 41 DC B1 3F 32 A6 52 F9 34 95 AB 68 2F ED BF 41 A7 4E 14 BF 4F E4 E8 EC 6E 14 CA 2B 92 78 BC 90 F8 CD BB D2 3D A8 90 18 C6 C4 0D E6 7D F9 76 2D ED C6 3A 59 E0 9B 84 B1 95 8C 8E 3F FE D4 1E C9 97 33 8C A1 09 38 11 2D 5A B7 1A 73 94 12 A7 18 50 9C B3 61 13 3B E2 B5 6B 19 0E 5F 7B 52 51 DD 1B FA 60 EB 23 1B EB 06 F8 D4 BE 99 0F FB F6 5B	5E A6 D7 8C 41 DC B1 3F 32 A6 52 F9 34 95 AB 68 2F ED BF 41 A7 4E 14 BF 4F E4 E8 EC 60 16 C8 2B 92 78 BC 90 F8 CD BB D2 3D A8 90 18 C6 C4 0D E6 7D F9 76 2D ED C6 3A 59 E0 9B 84 B1 95 8C 8E 3F FE D4 1E C9 97 33 8C A1 09 38 11 2D 5A B7 1A 73 94 12 A7 18 50 9C B3 61 13 3B E2 B5 6B 19 0E 5F 7B 52 51 DD 1B FA 60 EB 23 1B EB 06 F8 D4 BE 99 0F FB F6 5B	success or wait	1	32CB195	RegSetValueExA

Disassembly

No disassembly