ID: 878630
Sample Name: 15dasx.msi
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:54:44
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

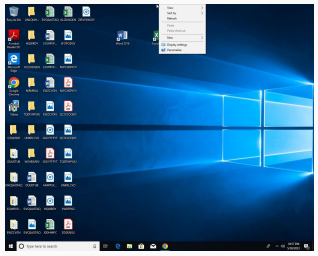
Windows Analysis Report

15dasx.msi

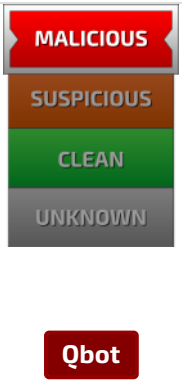
Overview

General Information

Sample Name:	15dasx.msi
Analysis ID:	878630
MD5:	ab8ef34233241..
SHA1:	a7e273ddd7cd…
SHA256:	4e70da2d2efc8..
Tags:	msi
Infos:	



Detection



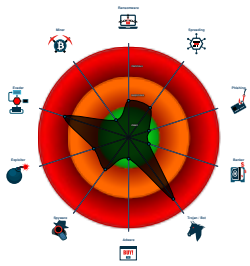
Qbot

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Qbot
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- 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
- Deletes files inside the Windows fol…

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 5760 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\15dasx.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 5708 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - rundll32.exe (PID: 5184 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 4028 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - wermgr.exe (PID: 6944 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - wscript.exe (PID: 1008 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": "BB30",
  "Campaign": "1685433861",
  "Version": "404.1320",
  "C2 list": [
    "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",
    "105.186.128.181:995",
    "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",
    "12.172.173.82:995",
    "77.86.98.236:443",
    "104.35.24.154:443",
    "213.64.33.61:2222",
    "47.149.134.231:443",
    "72.134.124.16:443",
    "47.34.30.133:443",
    "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",
    "188.28.19.84:443",
    "174.58.146.57:443",
    "94.207.104.225:443",
    "86.97.55.89:2222",
    "69.123.4.221:2222"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.554365630.000000000084A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000006.00000002.554539683.0000000001110000.00000004.00000020.00020000.00000000.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
6.2.rundll32.exe.fb0000.1.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
6.2.rundll32.exe.fb0000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
6.2.rundll32.exe.860830.0.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
6.2.rundll32.exe.860830.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
6.2.rundll32.exe.860830.0.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

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

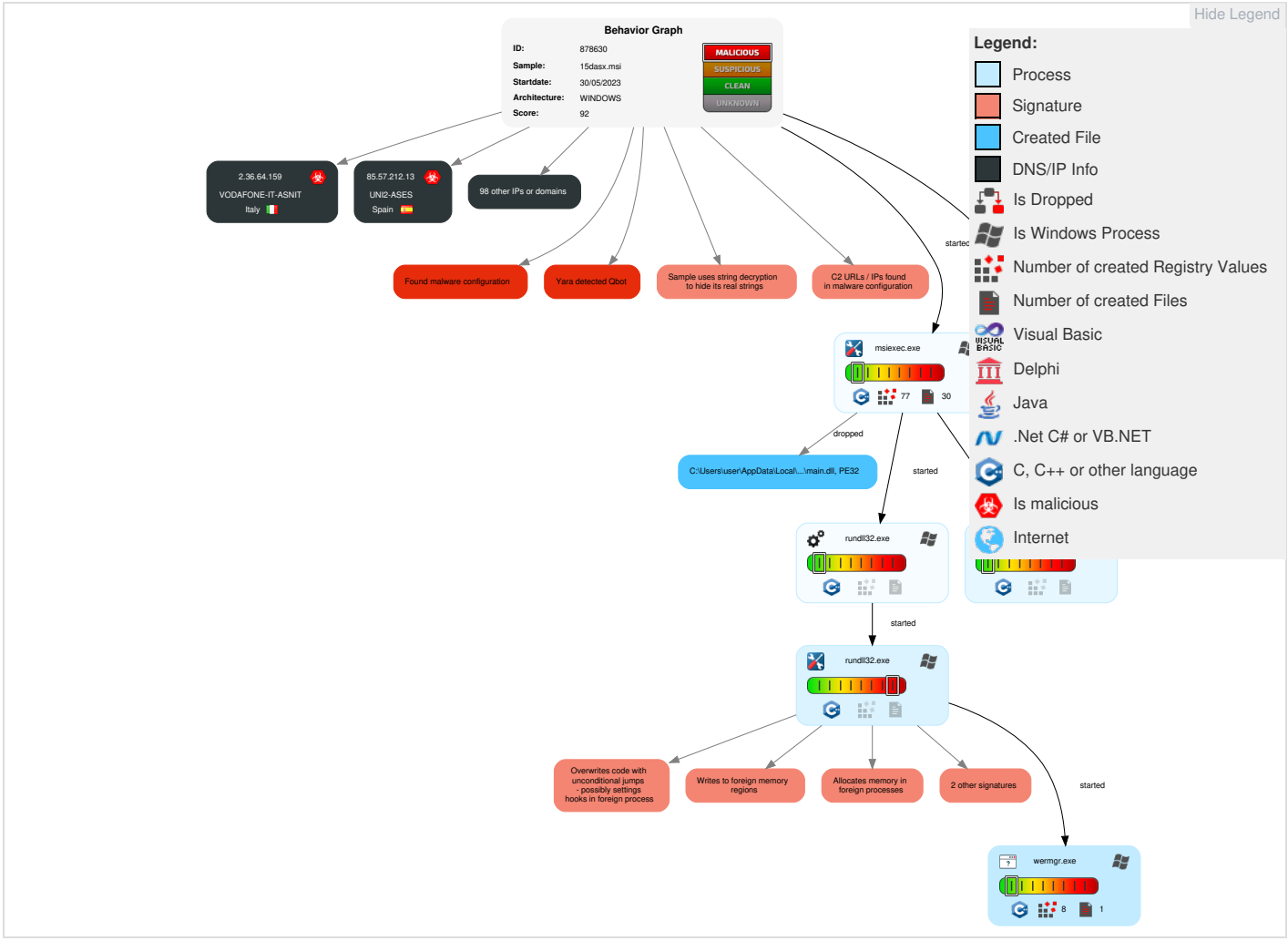
Yara detected Qbot

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 Masqueradi ng	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 Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	2 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	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	1 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)	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	2 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

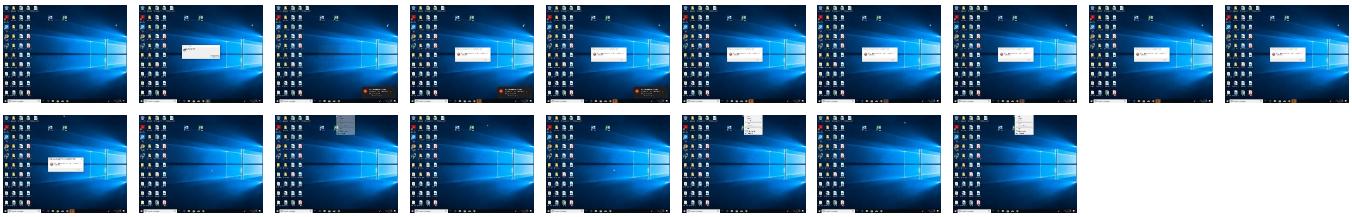
Behavior Graph



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
15dasx.msi	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

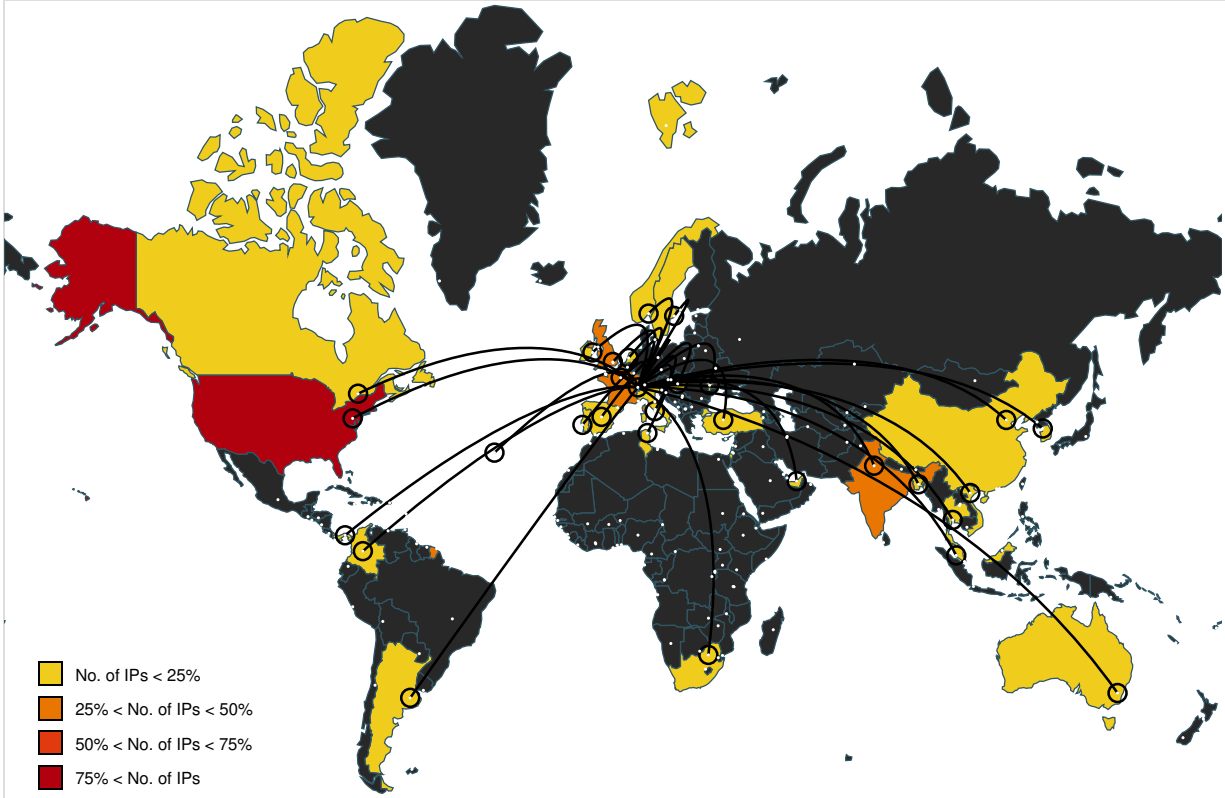
Contacted Domains

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, 00000006.00000002.554837079.00000000100AE000.00000002.00000001.01000000.00000005.sdmp, main.dll.2.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
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
14.192.241.76	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
173.88.135.179	unknown	United States		10796	TWC-10796-MIDWESTUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
124.149.143.189	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	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
59.28.84.65	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
105.186.128.181	unknown	South Africa		37457	Telkom-InternetZA	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
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
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
193.253.100.236	unknown	France		3215	FranceTelecom-OrangeFR	true
76.16.49.134	unknown	United States		7922	COMCAST-7922US	true
94.207.104.225	unknown	United Arab Emirates		15802	DU-AS1AE	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
47.149.134.231	unknown	United States		5650	FRONTIER-FRTRUS	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
86.97.55.89	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	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
104.35.24.154	unknown	United States		20001	TWC-20001-PACWESTUS	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
69.119.123.159	unknown	United States		6128	CABLE-NET-1US	true
69.123.4.221	unknown	United States		6128	CABLE-NET-1US	true
172.115.17.50	unknown	United States		20001	TWC-20001-PACWESTUS	true
77.86.98.236	unknown	United Kingdom		12390	KINGSTON-UK-ASGB	true

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

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878630
Start date and time:	2023-05-30 22:54:44 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
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:	8
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:	15dasx.msi
Detection:	MAL
Classification:	mal92.troj.evad.winMSI@10/21@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 5% (good quality ratio 2.2%) • Quality average: 19.7% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 89% • 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): audiodg.exe, WMIADAP.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- VT rate limit hit for: 15dasx.msi

Simulations

Behavior and APIs

Time	Type	Description
22:55:51	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\61e623.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	8918
Entropy (8bit):	5.58962421937737
Encrypted:	false
SSDEEP:	192:zXF6eaSEBwgr6SEBwgQH6NBIUVpy8T8amhl:z6rwPrwJc3i
MD5:	5E1B15017AF6242863525CEA042AE1E7
SHA1:	B1FFD512C754AA8AE9EA56A28E365C00119E6101
SHA-256:	4C9CFC15B5802B3FEFDB33C25095CD51A2DB9F1BCADF0F55AFBB4FC9A14AB7D9
SHA-512:	65FFC4E9437045D22CB345773768930DB4D97D195E08FBD2E89FA2F03E4D80991F6D8A9A87C3FC70C4E31B639C45BC80CAF933ED7F40CD435B1951C56493919
Malicious:	false
Preview:	...@IXOS.@.....@...V.@.....@.....@.....@.....@.....@.....&.{64EDF889-FC17-466B-8E9A-5A8688EB1CDC}'.Adobe Acrobat PDF Browser Plugin 4.8.25..15dasx.ms i.@.....@.....@.....@.....@.....&.{6ECD3C06-98A2-44A1-A41E-271C903F257F}.....@.....@.....@.....@.....@.....@.....@.....@....'.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}&.{64EDF889-FC17-466B-8E9A-5A8688EB1CDC}.@.....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\AppData\Local\AdobeAcrobatPDFBrowserPlugin\notify.vbs....WriteRegistryValues..Writing system registry values..Key: [1], Name: [2], Value: [3]$..@....%.Software\AdobeAcrobatPDFBrowserPlugin...@....(.&...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):	962048
Entropy (8bit):	6.7504689709982175
Encrypted:	false
SSDEEP:	24576:D7AkdHt+UnNtqbVotX4Dw/9JGCZdBK/+NYouXFPn/yd47:DZ8RDwlJGoY7X7
MD5:	A55C357391C089F93F5EF157BE209F63
SHA1:	A859A7AB02760EE8CD4DCF219EB1D460371350A8
SHA-256:	8D0C96718D4C7944FB648DF446D70ABBB87C5D4FF7C9735CF3BD9B2F11246A9E
SHA-512:	36152E39BACA8A0566C31DB97FF35D30E995FED246509C9816966D49F82143155225FE4BF07B7975DB1BEDC299008442FEC05D5A7588C18F6FD6EE1E821A471E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0d.....#...'.....0 .....{... ..@... .....hC.....0..x.....@..(A.....a.....(.....text...$.....`..`.data.....@....rdata..$.....@..@.bss....d.....`.....edata..hC.....D..`.....@..@.idata.....@....CRT....0.....@....tls..... .....@....rsrc...N....0.....@....reloc..(A.....B...I.....@..B.....

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\61e622.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: {6ECD3C06-98A2-44A1-A41E-271C903F257F}, Create Time/Date: Tue May 30 15:19:58 2023, Last Saved Time/Date: Tue May 30 15:19:58 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):	516096
Entropy (8bit):	7.918002678282303
Encrypted:	false
SSDEEP:	6144:jESkw7402pCiyBH6DIlxtWb9jOyHLmsjzcGet8Rghs0O892YptgrGzjkacDO+cDb:3kdiMHHLmKzQ8tfacDO+wVydjSavjQ
MD5:	AB8EF3423324168D06B2D122F75CA130
SHA1:	A7E273DDD7CDF303E366CBA16ABFD4C3966F2CF6
SHA-256:	4E70DA2D2EFC833EB5C450C9F82AAA7D433E31E39DC4EC36CA3C5DDDE0F4DC00
SHA-512:	8AADA720840A74A361D92DB1174D3AE8119FF2F70903A396BC0AE60ACFDFDF5D7FB781315B155F0B507B7B260A3F4FF8435DC9BA13E05F1547F2ABEA0C7DA220
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\61e624.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: {6ECD3C06-98A2-44A1-A41E-271C903F257F}, Create Time/Date: Tue May 30 15:19:58 2023, Last Saved Time/Date: Tue May 30 15:19:58 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):	516096
Entropy (8bit):	7.918002678282303
Encrypted:	false
SSDEEP:	6144:jESkw7402pCiyBH6DIlxtWb9jOyHLmsjzcGet8Rghs0O892YptgrGzjkacDO+cDb:3kdiMHHLmKzQ8tfacDO+wVydjSavjQ
MD5:	AB8EF3423324168D06B2D122F75CA130
SHA1:	A7E273DDD7CDF303E366CBA16ABFD4C3966F2CF6
SHA-256:	4E70DA2D2EFC833EB5C450C9F82AAA7D433E31E39DC4EC36CA3C5DDDE0F4DC00
SHA-512:	8AADA720840A74A361D92DB1174D3AE8119FF2F70903A396BC0AE60ACFDFDF5D7FB781315B155F0B507B7B260A3F4FF8435DC9BA13E05F1547F2ABEA0C7DA220
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSIE8E1.tmp	
Process:	C:\Windows\System32\msiexec.exe

File Type:	data
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	5.594517269430135
Encrypted:	false
SSDEEP:	48:uf1lnOLJwCP3PDufgL8YPRBoD8SY1eU/L4nLu1lnCnfaEVltdtc1ln2n:uXSx8YPrAuei4LeefaEP62n
MD5:	0B9D3C758584EFBC3D985C5162C20293
SHA1:	C52730B3195BB336B0EF282A2BD0156370E58946
SHA-256:	7258FD70ADEAA67C3FF2519AFD0B9B202A113D3E1A7CDB79AD14093211596014
SHA-512:	E7CE00C7CBD26543B17EE34BE456CAD607FCED4A8696670AA0FE36557EAB998AE92F731BC7F90DCD9CE43A3F3BC9BCB1711BCFA1F93969FB63F68E7D79877D6C
Malicious:	false
Preview:	...@IXOS.@.....@...V.@.....@.....@.....@.....@.....@.....&.{64EDF889-FC17-466B-8E9A-5A8688EB1CDC}'.Adobe Acrobat PDF Browser Plugin 4.8.25..15dasx.ms i.@.....@.....@.....@.....@.....&.{6ECD3C06-98A2-44A1-A41E-271C903F257F}.....@.....@.....@.....@.....@.....@.....@.....@....'.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\61e622.msi.....@.....main.dll..dll_main..main.dll.@.... .@.....@.....@...

C:\Windows\Installer\SourceHash{64EDF889-FC17-466B-8E9A-5A8688EB1CDC}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1628561562250028
Encrypted:	false
SSDEEP:	12:JSbX72FjSSAGiLIlHVRpth/77777777777777777777777vDHFPuC77HrpSI0G:JASQI5pFBHlF
MD5:	761F50755F94D674E4A0718AE489EEA6
SHA1:	376CD210E0C0A763F0275EB0FAFA81854D53CD4C
SHA-256:	C50AF6F0221FC0F08047984BD35891BC143B85051F0F713DF8FEDDF4459F8DB8
SHA-512:	0BFF860E332AC3E530CCA69FFDEB7CB65A942759984B0B1A9DE21B9609A099FE8684C9F776E51AEF9011AC2347030D1BB034C6EB6AAB24EF423CDE2946F2C889
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):	1.5046533420623267
Encrypted:	false
SSDEEP:	48:S8PhfuRc06WXJ8FT50zPHW9MS5o7rD6W9MSI818l:9hf1fFTaTjA
MD5:	F5A23A6FA744EEF09C2A7F8541FE5DBD
SHA1:	58DF694B007EF6DA2684EE80B1A150FBD06B1548
SHA-256:	3DA02C45DDA5D077670C8CDD0D85A7CEC4D36FB08AAAE3E70A8FA6A3E04CB15F
SHA-512:	79EF5CB1B4B46677FB0432A43533B0D7C6A2092BF627E5B9186BF067BB59CAFB9F6A82340BBD627780EC7A20811A3D746CC9D2F578A647A4D1EFDC2B5688F2B5
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):	79122

Entropy (8bit):	5.2821177886063175
Encrypted:	false
SSDEEP:	192:jmXs969ozNSkk3peTBYeHt0tfol9qsjl0urmwYyidu:yXs9UogeWeH29qclhmwYyidu
MD5:	F2FB6C9C2B6BE3CF826D2DBE6C29F575
SHA1:	8D7A1AB2F22024BD1E7F41506C05DAC7967EC6D8
SHA-256:	6DC9DFDE23D1421DDA60C7A94E25C4DE0024FCFE965CFA186EF5F55A085638DA
SHA-512:	10CE96B3726376A8956F5462C4DF497295574872976D52D3EFAFBE57EB89070570BBF3D5128785D11D92EE4DF14F784B1306970826DB34039114F23078B89D89
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 03:22:38.143 [320]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.159 [320]: ngen returning 0x00000000..07/23/2020 03:22:38.222 [3748]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Word, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.237 [3748]: ngen returning 0x00000000..07/23/2020 03:22:38.284 [64]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Common.Implementation, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.300 [64]:

C:\Windows\Temp\~DF0BFC98B297E831EB.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):	1.2093196290859516
Encrypted:	false
SSDEEP:	48:1sHugPveFXJxT5AzPHW9MS5o7rD6W9MSl818l:iHAJTWTjA
MD5:	18D15B6891825B20A3FBBD04738B6633
SHA1:	69E5E10D9DE4E4C3E0C9F4D9AD51C071228EB6B1
SHA-256:	5788AACC4AC4E19C88C167DE4CF4E160D4065A20C3A317FD96AD8DA3432ED381
SHA-512:	F052F7D843B69C8CECE9DFA8A683188C3CD1CB37E2457942E358F143D0C000F5F9124FE680F0A1A19745788E604CB934A74DB51D85A8FB5BA9F11A00152390A
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF1942D938D9238C10.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.12041817052530558
Encrypted:	false
SSDEEP:	24:Cr7l818lOdWm29qrb9ipVIdWm29qrb9ipV7V2BwG/IrkgX+Yre8:j818lEW9MSoW9MS5o7rXp1
MD5:	A5ACCD3443CED8BC0B4137E3EA396278
SHA1:	CCA264CCC071A3FCC3AEA76C934A3F9C313D61D4
SHA-256:	463244DE3829B3C5D994719E93594B2BB0BF9E382BBEEAE37E153BE97C8DED9E
SHA-512:	4F9B9577C32DB85762287074EBD87BE04D617AC15D9857613E1F81216B52BB14708D84EC2244D0BFB8DA8834B6EA1470EC622714D76366E1B80654ECE958BAC
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF1EBAA0DF6957A59B.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\~DF26625000C3DFA716.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):	1.2093196290859516
Encrypted:	false
SSDEEP:	48:1sHugPveFXJxT5AzPHW9MS5o7rD6W9MSl818l:iHAJTWTjA
MD5:	18D15B6891825B20A3FBBD04738B6633
SHA1:	69E5E10D9DE4E4C3E0C9F4D9AD51C071228EB6B1
SHA-256:	5788AACC4AC4E19C88C167DE4CF4E160D4065A20C3A317FD96AD8DA3432ED381
SHA-512:	F052F7D843B69C8CECE9DFA8A683188C3CD1CB37E2457942E358F143D0C000F5F9124FE680F0A1A19745788E604CB934A74DB51D85A8FB5BA9F11A00152390A
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DF515B98A092999243.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\~DF5DCD941B825AFF81.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):	1.5046533420623267
Encrypted:	false
SSDEEP:	48:S8PhfuRc06WXJ8FT50zPHW9MS5o7rD6W9MSl818l:9hf1fFTaTjA
MD5:	F5A23A6FA744EEF09C2A7F8541FE5DBD
SHA1:	58DF694B007EF6DA2684EE80B1A150FBD06B1548
SHA-256:	3DA02C45DDA5D077670C8CDD0D85A7CEC4D36FB08AAAE3E70A8FA6A3E04CB15F
SHA-512:	79EF5CB1B4B46677FB0432A43533B0D7C6A2092BF627E5B9186BF067BB59CAFB9F6A82340BBD627780EC7A20811A3D746CC9D2F578A647A4D1EFDC2B5688F2B 5
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFC281F47278832CCC.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\~DFD46BF27CA9C44E38.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):	1.2093196290859516
Encrypted:	false
SSDEEP:	48:1sHugPveFXJxT5AzPHW9MS5o7rD6W9MSl818l:iHAJTWTjA
MD5:	18D15B6891825B20A3FBBD04738B6633
SHA1:	69E5E10D9DE4E4C3E0C9F4D9AD51C071228EB6B1
SHA-256:	5788AACC4AC4E19C88C167DE4CF4E160D4065A20C3A317FD96AD8DA3432ED381
SHA-512:	F052F7D843B69C8CECE9DFA8A683188C3CD1CB37E2457942E358F143D0C000F5F9124FE680F0A1A19745788E604CB934A74DB51D85A8FB5BA9F11A00152390A
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFD92D1524EDDCFC25.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\~DFEAFD4A49B5364FC1.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):	1.5046533420623267
Encrypted:	false
SSDEEP:	48:S8PhfuRc06WXJ8FT50zPHW9MS5o7rD6W9MSl818l:9hf1fFTaTjA

MD5:	F5A23A6FA744EEF09C2A7F8541FE5DBD
SHA1:	58DF694B007EF6DA2684EE80B1A150FBD06B1548
SHA-256:	3DA02C45DDA5D077670C8CDD0D85A7CEC4D36FB08AAAE3E70A8FA6A3E04CB15F
SHA-512:	79EF5CB1B4B46677FB0432A43533B0D7C6A2092BF627E5B9186BF067BB59CAFB9F6A82340BBD627780EC7A20811A3D746CC9D2F578A647A4D1EFDC2B5688F2E5
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DFF6F31659CEE207E5.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\~DFFD8F8C1867A8E867.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.06981092353499595
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOzTuC77BhXKPQVky6lS:2F0i8n0itFzDHFPuC77HWS
MD5:	82E43552F0F7875FD425564DAB1C45C5
SHA1:	A85775C63AF567CCBCEECF01E8E10B3CB56661E7
SHA-256:	31D5DF542C7533A468E811F5E32ABD1B0988FC35D56A233FFC4CA4211202FB2A
SHA-512:	F1936D8774A71CF61F23D07D5076864EE447765BCEF5C00C6647EF8951C6CABA1486ADAD3C986A2C6904567D6601CE5C49DF990772ACFD19B5A071779659284
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: {6ECD3C06-98A2-44A1-A41E-271C903F257F}, Create Time/Date: Tue May 30 15:19:58 2023, Last Saved Time/Date: Tue May 30 15:19:58 2023, Number of Pages: 200, Number of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Entropy (8bit):	7.918002678282303
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	15dasx.msi
File size:	516096
MD5:	ab8ef3423324168d06b2d122f75ca130
SHA1:	a7e273ddd7cdf303e366cba16abfd4c3966f2cf6
SHA256:	4e70da2d2efc833eb5c450c9f82aaa7d433e31e39dc4ec36ca3c5ddde0f4dc00

SHA512:	8aada720840a74a361d92db1174d3ae8119ff2f70903a396bc0ae60acfdfdf5d7fb781315b155f0b507b7b260a3f4ff8435dc9ba13e05f1547f2abea0c7da220
SSDEEP:	6144:jESkw7402pCiyBH6DIlxtWb9jOyHLmsjzcGet8Rghs0O892YptgrGzjkacDO+cDb:3kdiMHHLmKzQ8tfacDO+wVydjSavjQ
TLSH:	DDB4231536022373C5014B72DC9D87ECA70A3E59756AB61F7E09F8480EB6B7D12B72A3
File Content Preview:	.....>.....

File Icon

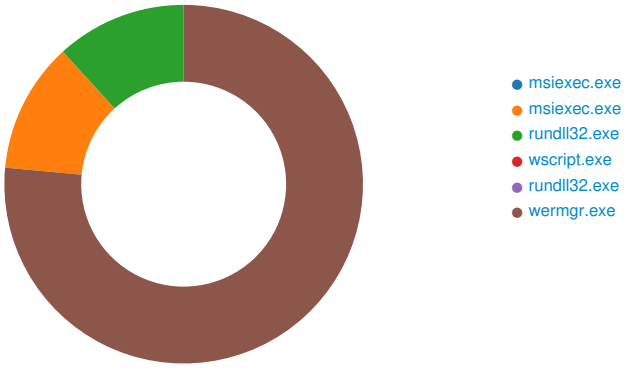
Icon Hash:	2d2e3797b32b2b99

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 5760, Parent PID: 3528

General

Target ID:	0
Start time:	22:55:39
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\15dasx.msi"
Imagebase:	0x7ff7d4ee0000
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: 5708, Parent PID: 576

General

Target ID:	2
Start time:	22:55:39
Start date:	30/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff7d4ee0000
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	79028	94	30 35 2f 33 30 2f 32 30 32 33 20 32 32 3a 35 35 3a 34 30 2e 39 34 34 20 5b 35 37 30 38 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 22:55:40.944 [5708]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FF8759DBEF0	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	7FF8759DBBC6	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: 5184, Parent PID: 5708

General	
Target ID:	4
Start time:	22:55:42
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:	0x7ff7004d0000
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	7FF7004D2FA7	ReadFile
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	264	success or wait	1	7FF7004D2FEA	ReadFile

Analysis Process: wscript.exe PID: **1008**, Parent PID: **5708**

General	
Target ID:	5
Start time:	22:55:42
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:	0x7ff68fed0000
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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **4028**, Parent PID: **5184**

General	
Target ID:	6
Start time:	22:55:42
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:	0x11b0000
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: 00000006.00000002.554365630.000000000084A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000006.00000002.554539683.0000000001110000.00000004.00000020.00020000.00000000.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: **6944**, Parent PID: **4028**

General

Target ID:	7
Start time:	22:55:46
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x7ff7c72c0000
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\Ywtarqug	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2E12CEB	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	962048	success or wait	2	2E1E746	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	success or wait	1	2E1AC70	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	bdbd51c2	binary	C7 61 5C 05 69 96 02 57 21 F0 D7 78 36 37 64 DA 37 36 E2 18 BA FB 33 D5 1F F3 8A 6A 97 02 56 B5 4D 22 11 AB 91 E8 4A DF 7D 7C 9D 61 4B FA 9B F4 B1 C4 AD A9 A8	success or wait	1	2E1B195	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	8822818c	binary	5E 8A 3B 49 E7 02 FB 54 EC 23 78 F7 8B 6B 6F 24 59 9E D7 1F 49 50 79 32 80 DB 40 DD E1 78 11 DE ED A0 3F DA 2E C7 51 32 79 7C DC 11 0B 88 8D DF 7A 3C 29 C5 90 07 A4 66 7E 53 0E D7 6F E8 64 F8 CF F5 D1 CB 81 3E DD 28 35 F3 8D 5E 54 7B 06 AE 17 24 01 2B FB 44 01 9B 20 1A BB C9 3C F4 A1 87 82 91 30 B7 FB 27 21 6F 29 F6 FE 04 7E 3C 85 3C CC 01 2C 11 E1 43 D6 A2 C1 63 06 04 AB C7 84 13 0E F0 F9 C6 61	success or wait	1	2E1B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	8a63a1f0	binary	23 E4 F0 EF 03 97 7C 2F 45 0A 89 47 15 8B A8 20 43 5B 3E 31 93 EA 72 5B DE F2 FF 31 AD CE 13 DB 02 39 11 DB 4E E7 48 E7	success or wait	1	2E1B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	32dfc695	binary	E1 84 E4 B8 2E 5A F7 27 A0 2C 23 E4 14 39 E0 09 F3 40 CA 73 76 94 25 85	success or wait	1	2E1B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	4fd7891f	binary	CA 7C 87 10 FE 34 CB 06 20 70 F8 75 44 A8 43 E5 20 A6 AB 27 AC 71 99 C5 7A 5B D4 83 C8 E6 9E F5 BD 2F A0 84 AA BC AD E0 30 40 00 C3 7D 20 97 58 42 04 9D	success or wait	1	2E1B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	f76bee7a	binary	79 DA 31 41 D1 12 22 E2 D4 8C F4 DE 25 6B A4 AD	success or wait	1	2E1B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	309ee6e9	binary	35 E6 F2 0B 8D 95 BB C0 68 D8 FA C0 E7 11 E2 86 0D CF 3B AA E8 B6 D9 4A 75 23 8C B6 16 F0 7C F6 19 4E 3B AB 9B C7 45 59 96 46 37 CF 07 3D 1D 35 37 E6 13 3D F8 34 F8 B1 CB DF AC 0D 5D E2 4F F3	success or wait	1	2E1B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	c2f43e34	binary	F3 F5 C8 FC 9A 16 B9 F6 A1 FF 6B 85 F3 30 4B 00 B7 52 3A F8 05 9A EB 87 CE E0 29 91 EF B4 15 54 AD 45 1F 6C A7 C5 1E 09 E5 FC DA 66 4F 87 D3 FE 10 57 4D 10 33 B2 61 8A E5 F6 B5 33 FF 90 7F 55 17 F1 4F 86 54 B3 6F DB 1D 0A 96 E4 80	success or wait	1	2E1B195	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	bdbd51c2	binary	C7 61 5C 05 69 96 02 57 21 F0 D7 78 36 37 64 DA 37 36 E2 18 BA FB 33 D5 1F F3 8A 6A 97 02 56 B5 4D 22 11 AB 91 E8 4A DF 7D 7C 9D 61 4B FA 9B F4 B1 C4 AD A9 A8	C7 61 47 05 69 96 33 2E 90 3B A5 1C 9F 7B C8 A1 FB A3 C4 FA 96 8D 47 F3 4C 2D C2 A5 1A 22 A9 62 7C C7 B5 05 19 65 68 1F E2 0F 9D 04 6F B2 8F 95 F8 46 55 3E F7 42 D3 5B 9D 44 DB 9F 05 BE 4F E6 FC 5E 2B 3C 12 43 95 90 6B 44 EB 56 5E A4	success or wait	1	2E1B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Afpioeosplyv	bdbd51c2	binary	C7 61 47 05 69 96 33 2E 90 3B A5 1C 9F 7B C8 A1 FB A3 C4 FA 96 8D 47 F3 4C 2D C2 A5 1A 22 A9 62 7C C7 B5 05 19 65 68 1F E2 0F 9D 04 6F B2 8F 95 F8 46 55 3E F7 42 D3 5B 9D 44 DB 9F 05 BE 4F E6 FC 5E 2B 3C 12 43 95 90 6B 44 EB 56 5E A4	C7 61 47 05 69 96 33 2E 90 3B A5 1C 9F 7B C8 A1 FB A3 C4 FA 96 8D 47 F3 4C 2D C2 A5 18 24 A6 62 7C C7 B5 05 19 65 68 1F E2 0F 9D 04 6F B2 8F 95 F8 46 55 3E F7 42 D3 5B 9D 44 DB 9F 05 BE 4F E6 FC 5E 2B 3C 12 43 95 90 6B 44 EB 56 5E A4	success or wait	1	2E1B195	RegSetValueExA

Disassembly

No disassembly