ID: 878465
Sample Name: r3zg12.msi
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:05:23
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

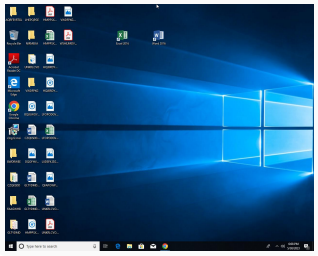
Windows Analysis Report

r3zg12.msi

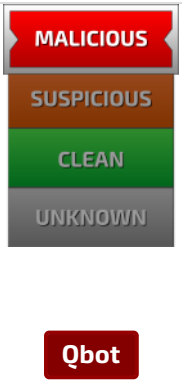
Overview

General Information

Sample Name:	r3zg12.msi
Analysis ID:	878465
MD5:	665afc8f8b797…
SHA1:	cc36e48f38375..
SHA256:	d764436caf711..
Tags:	msi
Infos:	



Detection



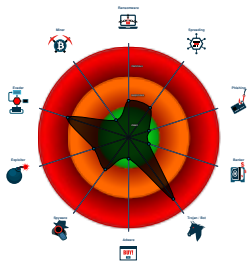
Qbot

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Qbot
- Overwrites code with unconditional j…
- C2 URLs / IPs found in malware con…
- Sample uses string decryption to hid…
- Potentially malicious time measurem…
- AV process strings found (often use…
- Queries the volume information (nam…
- Yara signature match
- PE file contains an invalid checksum
- Drops PE files
- Tries to load missing DLLs

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 7048 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\r3zg12.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 1948 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - rundll32.exe (PID: 3156 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 676 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - wermgr.exe (PID: 4340 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - wscript.exe (PID: 6980 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
00000004.00000002.374504814.0000000002D8A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000004.00000002.374584964.0000000004AB0000.00000004.00000020.00020000.00000000.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.2c90000.0.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.2c90000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.rundll32.exe.2da0830.1.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.2da0830.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.rundll32.exe.2da0830.1.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

Stealing of Sensitive Information

Yara detected Qbot

Remote Access Functionality

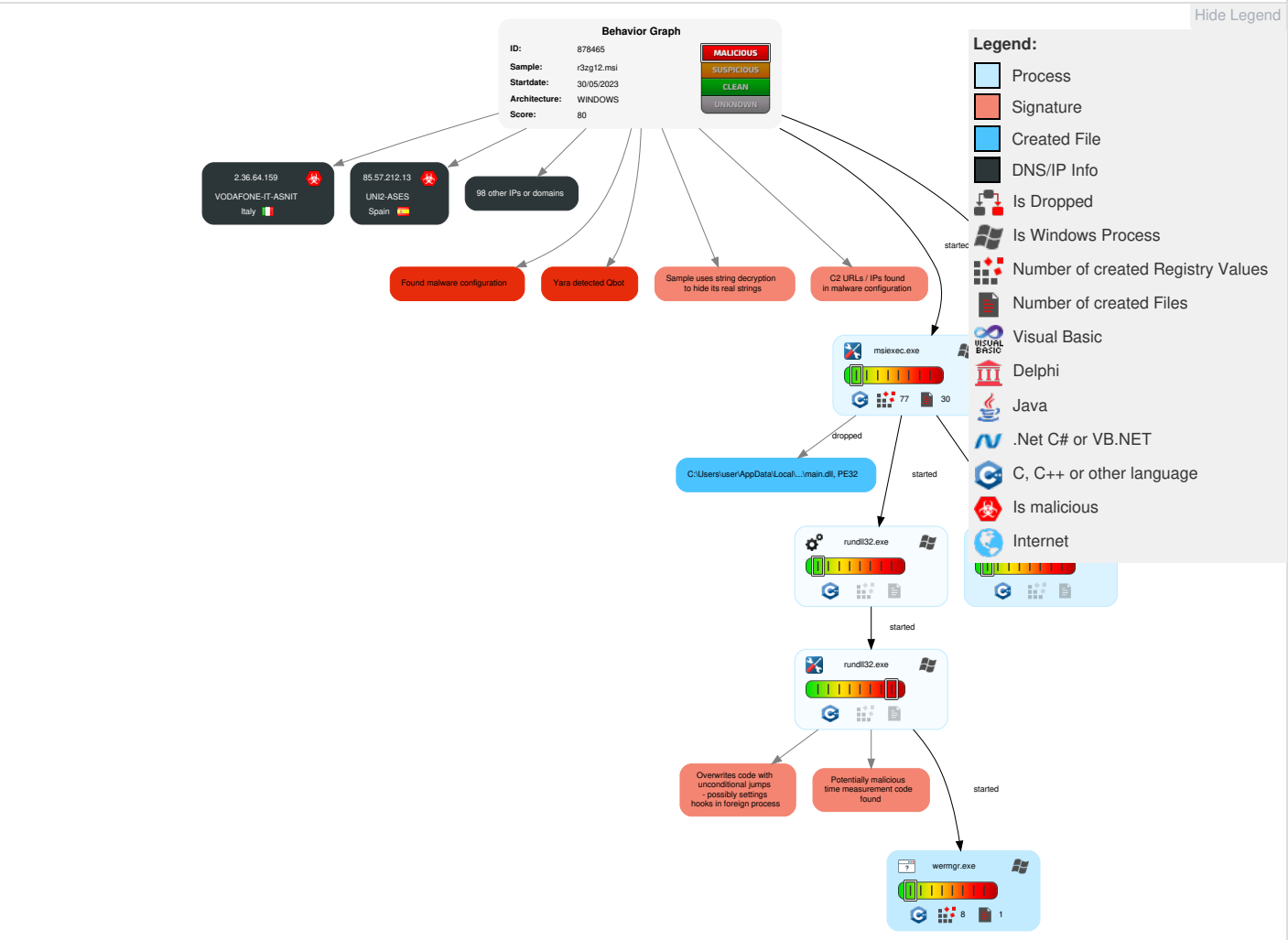
Yara detected Qbot

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	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	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	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 1 Scripting	LSA Secrets	1 1 Peripheral Device Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	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 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	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

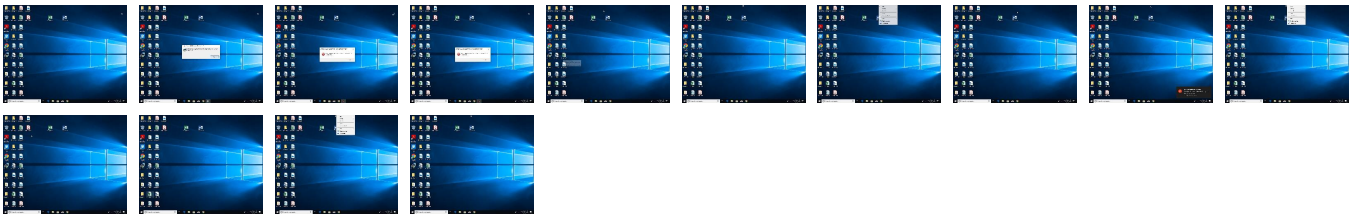
Behavior Graph



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
r3zg12.msi	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	3%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

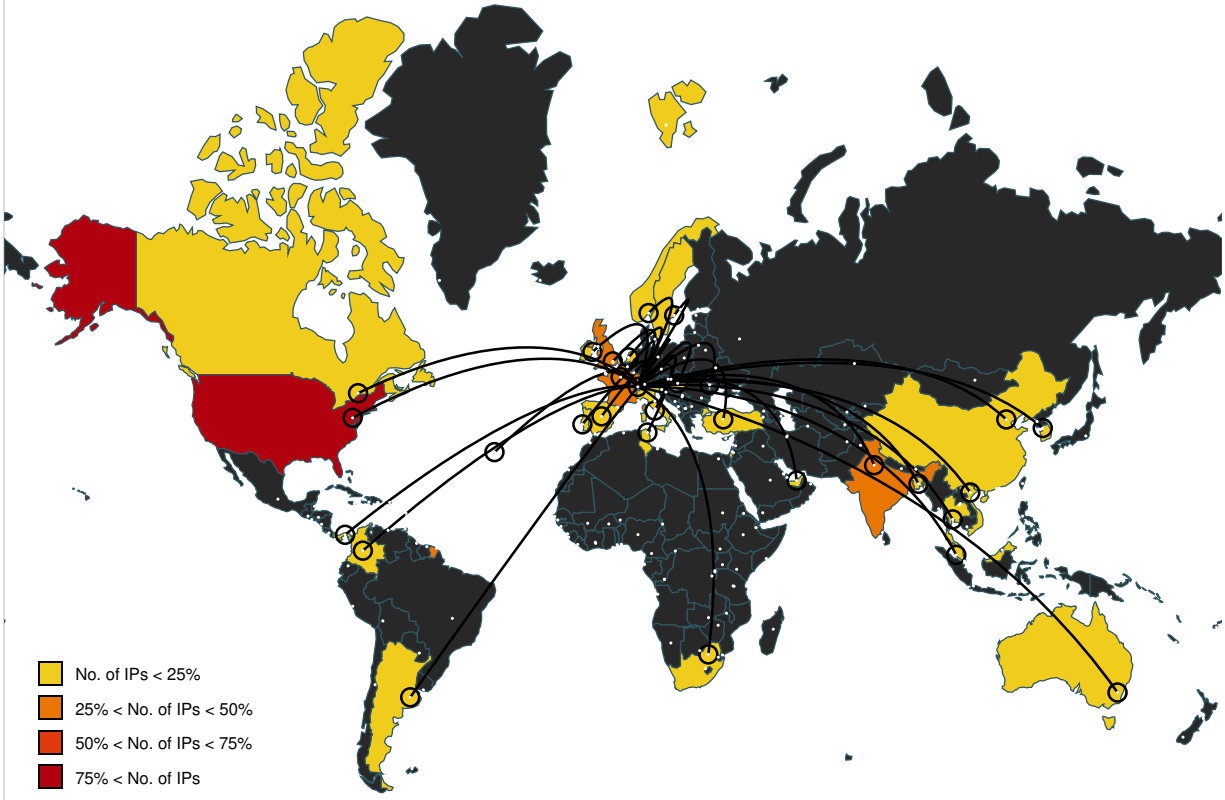
Contacted Domains

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, 00000004.00000002.374768576.00000000100AB000.00000002.00000001.01000000.00000003.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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
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:	878465
Start date and time:	2023-05-30 18:05:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 50s
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:	r3zg12.msi
Detection:	MAL
Classification:	mal80.troj.evad.winMSI@10/21@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15.6% (good quality ratio 7.1%) • Quality average: 20.6% • Quality standard deviation: 28.4%
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
18:06:29	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\5334e8.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	8918
Entropy (8bit):	5.546027034811531
Encrypted:	false
SSDEEP:	96:reeKeWZJS2URPw9CsvRqWURPw9C6jR8iU/vRqmHVPYaTNnohcw+n+PTLwCUVpTBs:rmejZwg3ZwgjlbQ3UVpW
MD5:	C812AA360AFC13D5A8C4449856D77BA8
SHA1:	CC95BB7FE63ECAA1B3B37AE30C6D2338AEB1DAB9
SHA-256:	4CFFB89764A8A7C0EDE2242FB8968A6A2F1EEEF03B881A3A788FAA0DFA1F824A
SHA-512:	AA60CBEC3A325A173D7E2406416320DDBFBE6E999829C37F36A541AF2FF8298AD8C668328BCFB3CDCA1BAE98334E762927A2ECB5CD8681BBFFBF55832BBE846A
Malicious:	false
Preview:	...@IXOS.@.....@..V.@.....@.....@.....@.....@.....@.....&.{BADFC54D-C40E-45B2-8055-C154444F1F83}'.Adobe Acrobat PDF Browser Plugin 4.8.25..r3zg12.msi.@.....@.....@.....@.....@.....@.....&.{880CDD59-0C2C-49AC-BA45-82BB01CD8BD1}.....@.....@.....@.....@.....@.....@.....@.....@....'.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}&.{BADFC54D-C40E-45B2-8055-C154444F1F83}.@.....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):	952832
Entropy (8bit):	6.765768694509863
Encrypted:	false

SSDEEP:	24576:UkgLxg2eMP8EN8Vo7zgDQ9uo4iZSBi/u3wXqx9jKVM5qx0YJ:x/jDQMo49wpq
MD5:	5E107608DD00957472DB2C1FCC77599D
SHA1:	D9BFA3E88CA0F86182CB84D4008AC6B346B755E9
SHA-256:	185737016A01E84BF88523A4681723B4F2D0D22520E77B76740CC3C6323E38BF
SHA-512:	22DFAE946F939EB361CEF49ED6EB953097A23A31BE0E97E6B7D31D3B2152C2371DA44E9E6BDD369E7145856BA75369FEA4DEAB18FA035E2A2CBD1E7D4E23CAF4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 3%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...m..d.....#...8..... ....@... .....hC.....<..... ...?.....$J.....text...4.....`.0`.data.....@.0..rdata..|.....@.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\5334e7.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: {880CD D59-0C2C-49AC-BA45-82BB01CD8BD1}, Create Time/Date: Tue May 30 14:29:16 2023, Last Saved Time/Date: Tue May 30 14:29:16 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):	7.919635795804226
Encrypted:	false
SSDEEP:	12288:vn+NgINNEcfjVRMigNFoILI8KviLjvhAN+S0w3:vnX9gjVRMDqH8fL1+35
MD5:	665AFC8F8B7972F427FE1BD90D263032
SHA1:	CC36E48F383750EB9416961B52EE3100B6E30688
SHA-256:	D764436CAF7114D880F982D208BD9514A433772DCAC851F27C510D1597E26EDD
SHA-512:	D30110DC240790A1F0C15DF31069D361F80DF327C258DD3305E70EB9EE3814C285AB6290E88E4072B375F7DAC3D183D22ABA29CB94FDD7DB937C4399C18AD3E
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\5334e9.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: {880CD D59-0C2C-49AC-BA45-82BB01CD8BD1}, Create Time/Date: Tue May 30 14:29:16 2023, Last Saved Time/Date: Tue May 30 14:29:16 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):	7.919635795804226
Encrypted:	false
SSDEEP:	12288:vn+NgINNEcfjVRMigNFoILI8KviLjvhAN+S0w3:vnX9gjVRMDqH8fL1+35

MD5:	665AFC8F8B7972F427FE1BD90D263032
SHA1:	CC36E48F383750EB9416961B52EE3100B6E30688
SHA-256:	D764436CAF7114D880F982D208BD9514A433772DCAC851F27C510D1597E26EDD
SHA-512:	D30110DC240790A1F0C15DF31069D361F80DF327C258DD3305E70EB9EE3814C285AB6290E88E4072B375F7DAC3D183D22ABA29CB94FDD7DB937C4399C18AD3E
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSI36EA.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	5.5791150458185745
Encrypted:	false
SSDEEP:	48:ZsT5zj3JwCP3RDufgFYjRBoD8SY1eU/rn7fnVaEVlt+Xt6q:G/hYjrAueIBaEP6
MD5:	1F6513D8FA2AB1C6046B39CC245944A4
SHA1:	B10AB5ACCE2B699F17C849407F8C3E7B3B1B8AFB
SHA-256:	DB342F3508603862C738AA37C27F04FA57E10FFD7C165662DC2FE04DEF7BE192
SHA-512:	71ECE8BDE50D6C91A79E43E3A3EDEC9B8B8B0B715ED7B5B0E20B82BC9845B28BC1B8981714876FCDA7BCEFEDE2A68C310C78528D5A58EBF54106589FE909A8CB
Malicious:	false
Preview:	...@IXOS.@.....@..V.@.....@.....@.....@.....@.....@.....&.{BADFC54D-C40E-45B2-8055-C154444F1F83}'.Adobe Acrobat PDF Browser Plugin 4.8.25..r3zg12.msi.@.....@.....@.....@.....@.....&.{880CDD59-0C2C-49AC-BA45-82BB01CD8BD1}.....@.....@.....@.....@.....@.....@.....@.....@....'.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\5334e7.msi.....@.....main.dll..dll_main..main.dll.@.....@.....@.....@...

C:\Windows\Installer\SourceHash{BADFC54D-C40E-45B2-8055-C154444F1F83}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1624552326555946
Encrypted:	false
SSDEEP:	12:JSbX72FjQAGiLIlHVRpth/77777777777777777777777vDHFZRwpSl0i8Q:JCQI5p0F
MD5:	37AB2087D8192F73564465B95F0BDA79
SHA1:	1406A27DC80D84250F76BF21BD56687AC594249F
SHA-256:	9D7BD6336C836A1991242C4A183A064021894E9A9F38F8CC6081274863C54DA7
SHA-512:	BBE40C0FAAB13636E98612B8805A8516026C839567AC998224CC8F8998E7A375E488E8DD33908401CEF9FC62CBB9A6D8F8F7100001E7205F90B449EFB8740948
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):	1.5060877643473185
Encrypted:	false
SSDEEP:	48:58PhfuRc06WXJ8FT5K0gMPduLMS5kArD6uLMSI818lP7AWMN:0hf1fFT3TPRtfA
MD5:	430F2ADF3561DDB478079AF68E971D68
SHA1:	7431BA57FB0275B6276BBA7370A317D67552D8B6
SHA-256:	8A709B97AFBFAA9E5CD5D3C566F95D370FE69AC31260A6F3C2FF82619F3D1026
SHA-512:	5A3904A81D986EE27F31D27383BB70BE01C709BFF580B7CD2AF184F8C8539439A3F38821B5C0D32B42F57DF0B92BC771B5ED7264082F842D19F346D3667C669A

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):	5.392009325809667
Encrypted:	false
SSDEEP:	3072:iHHJCoX5CNWFHjkzRl1pqf5JjzH6wbxygaK8Nkv6kF8Kwu8K8uBD556GIlZZ6bFd:i0LVlAb
MD5:	3B520410F621CAAC0C856D080A24DC73
SHA1:	62B660B648C06F16DFDEE47AC468EF44F9E81D14
SHA-256:	D71D62F7FA3DAF2E96B31CF428170D103C5D17C9326C1BCA9805C6FA561F2F40
SHA-512:	412F894D897944A54401373C827D06E0C7A48F63B809E3441EE8B8ABDBFA19F5A6B0C8C0A3E8FDDF9DD32BB6051623C5C404DEB241C993BE50CE8DDBBABAB 50C
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\~DF09B6AE6DA39A576A.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\~DF29580D728BC5B4ED.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.12071429906577896
Encrypted:	false
SSDEEP:	24:jIAWMQQt70R818lOdWmOLqrb9ipVIdWmOLqrb9ipV7VO3wGolrkgra+vMsvKL:cAWMN+R818lEuLMSouLMS5kArragMs
MD5:	5A66F5FD08B8CA2249380DDDF49D9D33
SHA1:	B4BD32E998A3A44BCC463E516596546E00296F96
SHA-256:	7825ED9BF119F45394DD851AAE50644AF5B0A10637237F55A7611CCCBDCCB99A
SHA-512:	4B13BD300E31411552873C292F037754D0D40AB5B9AA9941463F9A82099C4CABE7EE3B019753FB57046925FD63006A78B3941B0CF4FEC5EC663AA33F4DB13166
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF385081A1CE239BA3.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):	1.209919737144819
Encrypted:	false
SSDEEP:	48:rsHugPveFXJxT5+0gMPduLMS5kArD6uLMSI818lP7AWMN:IHAJTrTPRtfA
MD5:	5F8C47B7D4AFB1220F17DA429EAACB81
SHA1:	14180142867FDD137664D86CE077E44BB66C5DF9
SHA-256:	99A8B2F8F6B46ABADD467B39C55BECCE99C50AD04E3CCD0C5238548AA14257F7
SHA-512:	C7E3E848B867F1309B56B7F273434C906AF6ACF854A486B52A3B66C233976592DA52692535AD3E6C3B4D16A0AE46F7C7FB2A18707F056B95840781F73719CDDD
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF3DD2B7692E631D41.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):	1.209919737144819
Encrypted:	false
SSDEEP:	48:rsHugPveFXJxT5+0gMPduLMS5kArD6uLMSI818lP7AWMN:IHAJTrTPRtfA
MD5:	5F8C47B7D4AFB1220F17DA429EAACB81
SHA1:	14180142867FDD137664D86CE077E44BB66C5DF9
SHA-256:	99A8B2F8F6B46ABADD467B39C55BECCE99C50AD04E3CCD0C5238548AA14257F7
SHA-512:	C7E3E848B867F1309B56B7F273434C906AF6ACF854A486B52A3B66C233976592DA52692535AD3E6C3B4D16A0AE46F7C7FB2A18707F056B95840781F73719CDDD
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF4C3BF86A9825BAFE.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):	1.209919737144819
Encrypted:	false
SSDEEP:	48:rsHugPveFXJxT5+0gMPduLMS5kArD6uLMSI818lP7AWMN:IHAJTrTPRtfA
MD5:	5F8C47B7D4AFB1220F17DA429EAACB81
SHA1:	14180142867FDD137664D86CE077E44BB66C5DF9
SHA-256:	99A8B2F8F6B46ABADD467B39C55BECCE99C50AD04E3CCD0C5238548AA14257F7
SHA-512:	C7E3E848B867F1309B56B7F273434C906AF6ACF854A486B52A3B66C233976592DA52692535AD3E6C3B4D16A0AE46F7C7FB2A18707F056B95840781F73719CDDD
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF5DF60473004ABCC7.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\~DF6B3BC2C5354ED014.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\~DF7864E6E6496DBA61.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):	1.5060877643473185
Encrypted:	false
SSDEEP:	48:58PhfuRc06WXJ8FT5K0gMPduLMS5kArD6uLMSl818lP7AWMN:0hf1fFT3TPRtfA
MD5:	430F2ADF3561DDB478079AF68E971D68
SHA1:	7431BA57FB0275B6276BBA7370A317D67552D8B6
SHA-256:	8A709B97AFBFAA9E5CD5D3C566F95D370FE69AC31260A6F3C2FF82619F3D1026
SHA-512:	5A3904A81D986EE27F31D27383BB70BE01C709BFF580B7CD2AF184F8C8539439A3F38821B5C0D32B42F57DF0B92BC771B5ED7264082F842D19F346D3667C669A
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DF8AE2E68986D61390.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\~DF934EA1F7B18385F5.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\~DFC5E20CC9F13FECB6.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):	1.5060877643473185
Encrypted:	false
SSDEEP:	48:58PhfuRc06WXJ8FT5K0gMPduLMS5kArD6uLMSl818lP7AWMN:0hf1fFT3TPRtfA
MD5:	430F2ADF3561DDB478079AF68E971D68
SHA1:	7431BA57FB0275B6276BBA7370A317D67552D8B6
SHA-256:	8A709B97AFBFAA9E5CD5D3C566F95D370FE69AC31260A6F3C2FF82619F3D1026
SHA-512:	5A3904A81D986EE27F31D27383BB70BE01C709BFF580B7CD2AF184F8C8539439A3F38821B5C0D32B42F57DF0B92BC771B5ED7264082F842D19F346D3667C669A
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFDD7490D2FF8A1B23.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.06947604271114201
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOGljlnucCRjQVky6lS:2F0i8n0itFzDHFZRRS
MD5:	D429E7962EAB07E07C545C296E8B0F35
SHA1:	9AC331509B3E15434194BAECFA89488D380435FC
SHA-256:	14064733FE0126C92AE648CE46DD3AF9820F19CA4F87B6FFCD9134C3A4FD19EE
SHA-512:	BF7726A85BAFFE69B531188332BBE26F1ADFF215BAB9CB3FFA26B2FC1A6D6D337328E1670526C5040AF4C6F39E838456DE85834EBB97A704A641A7613297025
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: {880CD D59-0C2C-49AC-BA45-82BB01CD8BD1}, Create Time/Date: Tue May 30 14:29:16 2023, Last Saved Time/Date: Tue May 30 14:29:16 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):	7.919635795804226
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	r3zg12.msi
File size:	507904
MD5:	665afc8f8b7972f427fe1bd90d263032
SHA1:	cc36e48f383750eb9416961b52ee3100b6e30688
SHA256:	d764436caf7114d880f982d208bd9514a433772dcac851f27c510d1597e26edd
SHA512:	d30110dc240790a1f0c15df31069d361f80df327c258dd3305e70eb9ee3814c285ab6290e88e4072b375f7dac3d183d22aba29cb94fdd7db937c4399c18ad37e
SSDEEP:	12288:vn+NgINNEcfjVRMigNFoILI8KviLjvhAN+S0w3:vnX9gjVRMDqH8fL1+35
TLSH:	21B42359660A6371C4C826B2E73E77CFAAA27C5507038433C33B72DE1D775B81A663A1
File Content Preview:	.....>.....

File Icon

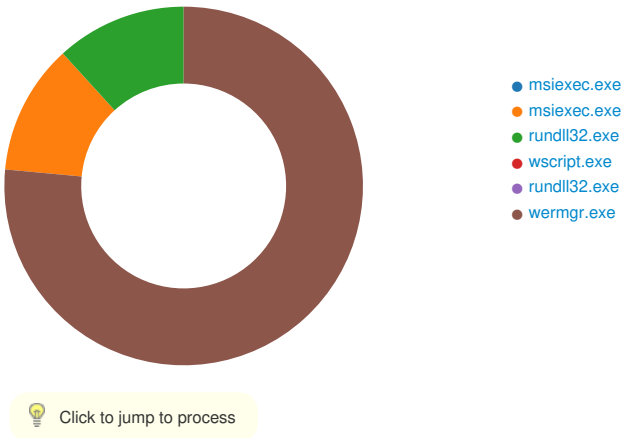
Icon Hash:	2d2e3797b32b2b99

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: msiexec.exe PID: 7048, Parent PID: 3452

General

Target ID:	0
Start time:	18:06:19

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\r3zg12.msi"
Imagebase:	0x7ff729140000
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: **1948**, Parent PID: **580**

General

Target ID:	1
Start time:	18:06:19
Start date:	30/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff729140000
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 31 38 3a 30 36 3a 32 30 2e 33 34 32 20 5b 31 39 34 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 18:06:20.342 [1948]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFC0B72BEF0	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	7FFC0B72BBC6	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: **3156**, Parent PID: **1948**

General

Target ID:	2
Start time:	18:06:21
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:	0x7ff709920000
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	7FF709922FA7	ReadFile
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	264	success or wait	1	7FF709922FEA	ReadFile

Analysis Process: wscript.exe PID: **6980**, Parent PID: **1948**

General

Target ID:	3
Start time:	18:06:21
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:	0x7ff715d10000
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: **676**, Parent PID: **3156**

General	
Target ID:	4
Start time:	18:06:21
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:	0x80000
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: 00000004.00000002.374504814.0000000002D8A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.374584964.0000000004AB0000.00000004.00000020.00020000.00000000.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: 4340, Parent PID: 676

General	
Target ID:	5
Start time:	18:06:24
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x50000
File size:	191904 bytes
MD5 hash:	CCF15E662ED5CE77B5FF1A7AAE305233
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Qiiyv	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2782CEB	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	278E746	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	success or wait	1	278AC70	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	d05a95f2	binary	54 5A 33 48 4A 8A 6B 46 9E DC 6B EB FE E6 9C 09 31 F3 EA A5 B4	success or wait	1	278B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	e5c545bc	binary	BA 55 1B 7C 3D 14 61 C3 26 41 F5 80 CB 13 AA 8D C2 F2 E5 E0 05 C1 2E 72 F1 AC 79 79 19 A9 28 66 2D 2D 1F 3F BF 6A 53 E6 EE 1E 86 33 76 49 F5 7F 14 E2 B6 9F 87 3B 4D 6C 39 33 77 A7 87 F7 0F 1A 60 5B 72 69 07 F2 A0 3D 2B F4 27 9E 38 19 39 31 65 FC FB 7E 3D 3B 7F 18 07 48 BF 8F B8 CB 79 E3 B9 CC 6D 2B 36 47 FF F1 47 10 0A D1 74 25 0B 07 8F C0 EF 93 73 96 3D 5D 64 37 69 CB BB B2 8C 0B 04 37 18 56 0A DB 9A C5 9A 63 B2 D3 39 C8 0F 4A 09 BE D2 A4 2F 17 78 DA 73 39 A1 09 2D 4A 68 14 D9 47 31 1B D4 74 A7 0A 69 4F CA 80 7C 29 73 C4 5A 96 D0 BF E9 8F 58 FE 02 78 B5 6F 11 BD AF 84 7B F4 5A BC 3B 46	success or wait	1	278B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	e78465c0	binary	7D 77 E9 8A 12 08 1A 6D 2C FF F5 1A 63 A8 90 03 D8 75 E1 95 29 34 62 3B 23 0B E2 87 2F 59 1D 59 F9 32 44 C1 F4 93 C1 4A E0 C9 26 88 89 0F 7B B2 8E B7 95 62 46 D5 8D F2 81 C5 40 71	success or wait	1	278B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	5f3802a5	binary	BE E1 39 8C 9A 3E FB CA A3 FC 04 D1 8F 36 9F 3B E1 97 40 22 EB 42 69 2B AE 2D F8 EE 6D 80 31 5C D6 5E 08 E5 6B 59 21 0C 29 9B 12 CC A2 0C BB BD 36 FB CC 8C B2 49 2F B7 DB 31 51 9A 75 AB C3 20 CF 84 C3 DA 3C FA B7 C4 55 34 E6 85 0E 30 BA 0E 0C F2 87 72 C7 61 75 BD 28 71 94 3A 72 A1 DC 8A 5F 3C F4 7F 67 73 9B 73	success or wait	1	278B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	22304d2f	binary	02 34 BD F1 6E B4 AD 83 D8 2D 58 EB B3 47 A1 69 22 12 47 1D 92 25	success or wait	1	278B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	9a8c2a4a	binary	82 AE ED BB B5 3D C9 F4 F6 FD 2C 86 30 7C C7 21 50 DA 8F 41 8C 59 1F 7D A1 15 26 5D AE 85 82 D1 64 3E 0D C4 2E 57 AC 74 3D B0 7A 4E 4A 1A 0E 02 2A ED 04 7E 2C 40 60 F5 14 A7 B8 CD FC 9C 81 03 00 39 94 1C A4 3E DE E5 32 55 E7 00 7F 02 C0 A6 C3 C3 2B 41 49 AE 3D 81 44 0D F5 56 91	success or wait	1	278B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	5d7922d9	binary	83 A9 60 94 E7 7B 1B 67 D4 6C 22 C0 F7 FB EC C6 30 82 FB 15 7D 00 E0 CB ED BB 98 A3 2D 3D 49 11 45 16 10 A9 3A 1F B2 CB A3 88 F6 0D 30 8E F1 0B 07 AB EC 78 EF 7A E9 12 92 77 94 31 63 3E 1C 04 CB 55 FB 4F D2 C2 05 00 D5 EF E0 AF 64 CB BB 65 A9 E8 43 72 58 B3 D0 7E 69 21 9E FA 68 C8 78 5A FD A2 C2 71 F4 49	success or wait	1	278B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	af13fa04	binary	C6 FF BA CD 69 B8 D0 55 43 7E AD 21 BB EE 39 1E 1F FB FD 3B C4 E4 E1 A8 14 66 81 FD 98 C5 1C 4D BB 31 14 AF 06 B5 0C 66 91 BE A4 56 2D 2A 64 FA 83 67 0A E6 8C 03 A9 3D 26 7D 33 F1 9F 66 3F 63 83 8D F5 11 84 10 8D 05 14 16 9B D4 FD 84 0D 33 8C 78 2B 34 72 ED 02 61 C1	success or wait	1	278B195	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\lwzhphvqnftb	d05a95f2	binary	54 5A 33 48 4A 8A 6B 46 9E DC 6B EB FE E6 9C 09 31 F3 EA A5 B4	54 5A 28 48 4A 8A 5A 65 59 41 5D 90 02 48 94 70 F0 C6 68 F0 80 BC A3 9B 33 E3 14 FB CC A6 9C 9A C6 23 AB 36 BD D9 2B C6 25 BA A5 E5 CE B9	success or wait	1	278B195	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Iwzhphvqnftb	d05a95f2	binary	54 5A 28 48 4A 8A 5A 65 59 41 5D 90 02 48 94 70 F0 C6 68 F0 80 BC A3 9B 33 E3 14 FB CC A6 9C 9A C6 23 AB 36 BD D9 2B C6 25 BA A5 E5 CE B9	54 5A 28 48 4A 8A 5A 65 59 41 5D 90 02 48 94 70 F0 C6 68 F0 80 BC A3 9B 33 E3 14 FB CE A8 9F 9A C6 23 AB 36 BD D9 2B C6 25 BA A5 E5 CE B9	success or wait	1	278B195	RegSetValueExA

Disassembly

No disassembly