ID: 878465
Sample Name: r3zg12.msi
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:55:55
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

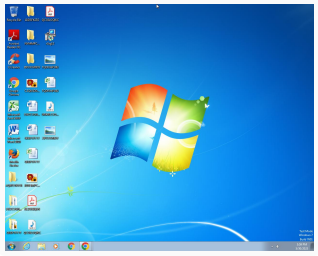
Windows Analysis Report

r3zg12.msi

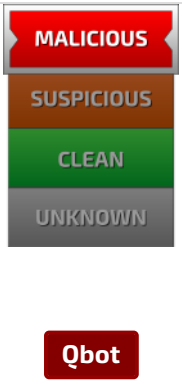
Overview

General Information

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



Detection



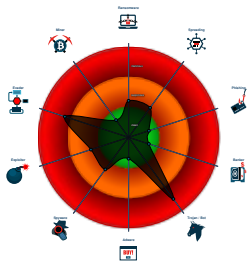
Qbot

Score:	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 w7x64**
- msiexec.exe (PID: 2364 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\r3zg12.msi" MD5: AC2E7152124CEED36846BD1B6592A00F)
- msiexec.exe (PID: 2184 cmdline: C:\Windows\system32\msiexec.exe /V MD5: AC2E7152124CEED36846BD1B6592A00F)
  - rundll32.exe (PID: 3244 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 3260 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 3332 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: C9905EA4C326DAB778B9297BA5BD1889)
  - wscript.exe (PID: 3252 cmdline: wscript.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\notify.vbs MD5: 045451FA238A75305CC26AC982472367)
- **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.pdfhttps://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"
```

```
      "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
00000007.00000002.1071797162.000000000029D000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000007.00000002.1072022431.0000000000E3D000.00000004.00000020.00020000.00000000.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
7.2.rundll32.exe.1c0000.0.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
7.2.rundll32.exe.1c0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
7.2.rundll32.exe.2aa328.1.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
7.2.rundll32.exe.2aa328.1.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
7.2.rundll32.exe.2aa328.1.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

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

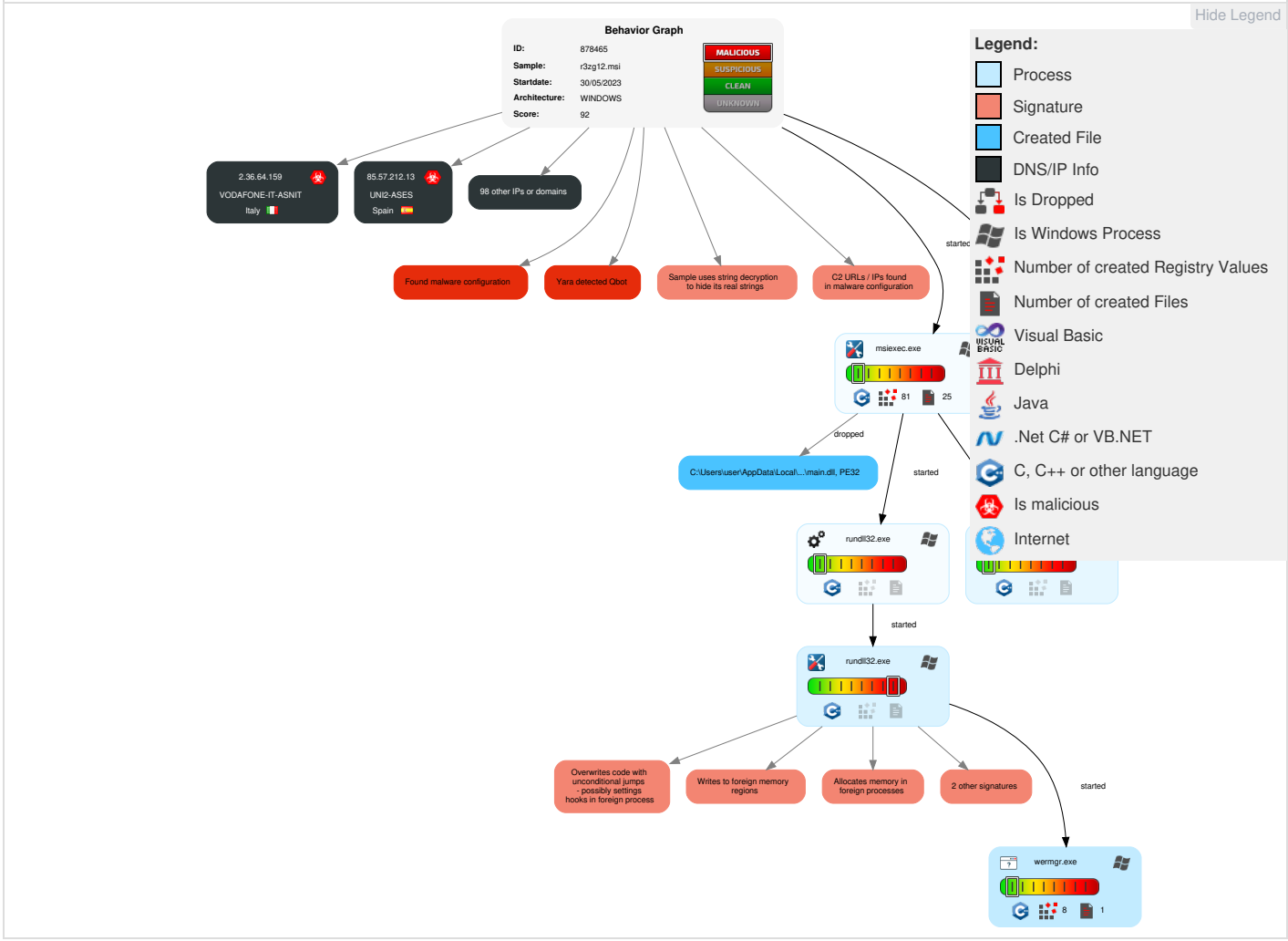
Yara detected Qbot

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	2 Windows Service	2 Windows Service	1 1 Masqueradi ng	1 Credential API Hooking	1 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	Scheduled Task/Job	Boot or Logon Initialization Scripts	3 1 1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 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	2 Obfuscated Files or Information	Cached Domain Credentials	2 3 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 Rundll32	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

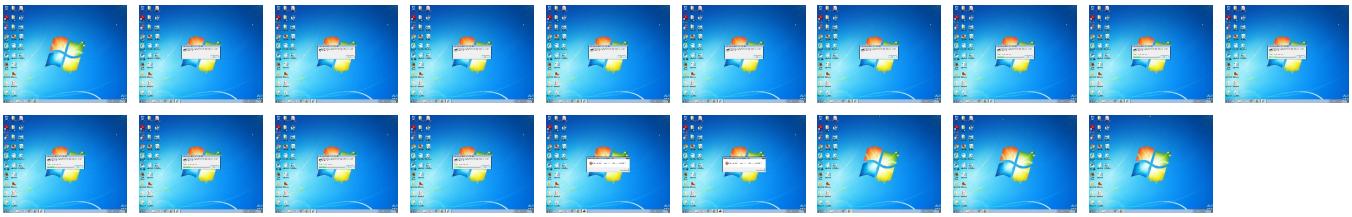
Behavior Graph



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		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

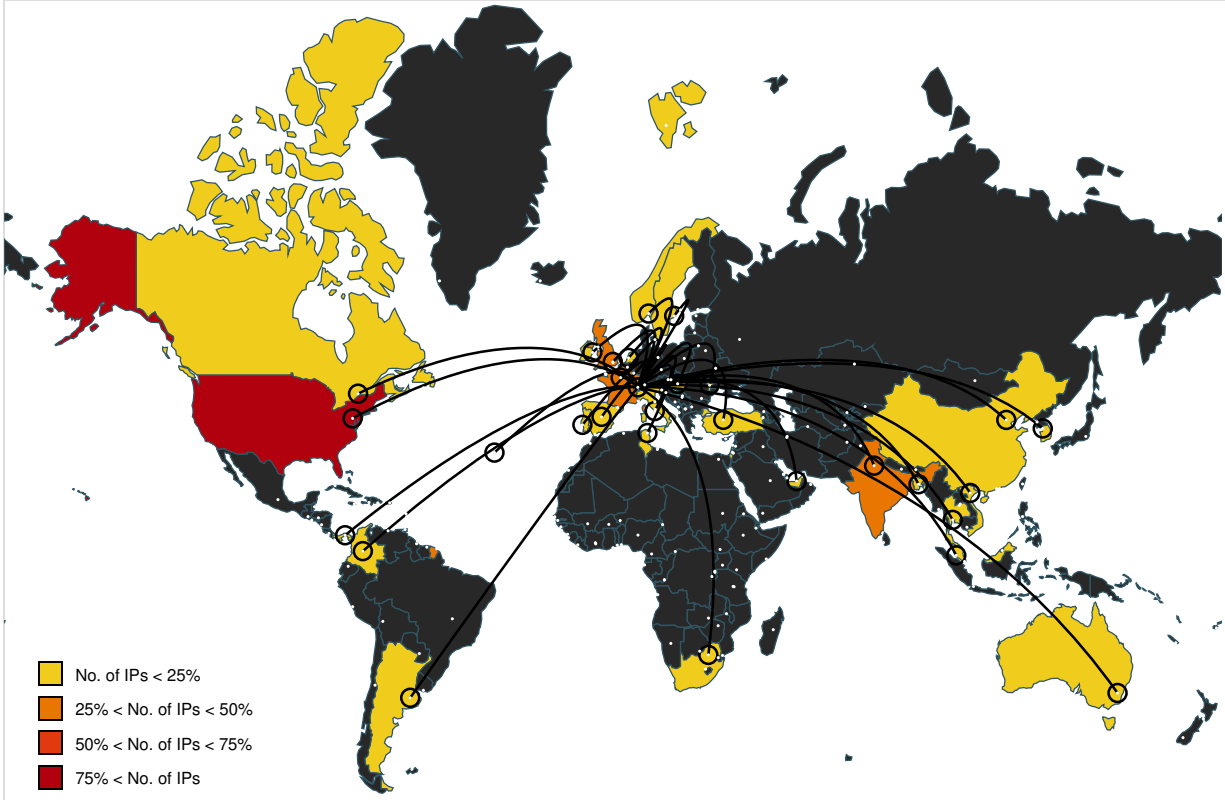
Contacted Domains

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, 00000007.00000002.1072236585.00000000100AB000.00000002.00000001.01000000.00000006.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

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
81.111.108.123	unknown	United Kingdom		5089	NTLGB	true
69.133.162.35	unknown	United States		11426	TWC-11426-CAROLINASUS	true
86.132.236.117	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
151.62.238.176	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
70.112.206.5	unknown	United States		11427	TWC-11427-TEXASUS	true
41.228.224.161	unknown	Tunisia		37693	TUNISIANATN	true
205.237.67.69	unknown	Canada		11290	CC-3272CA	true
102.159.188.125	unknown	Tunisia		37705	TOPNETTN	true
151.65.167.77	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
76.178.148.107	unknown	United States		10838	OCEANIC-INTERNET-RRUS	true
89.36.206.69	unknown	Italy		48544	TECNOADSL-ASIT	true
69.242.31.249	unknown	United States		7922	COMCAST-7922US	true
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
71.38.155.217	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
220.240.164.182	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
24.198.114.130	unknown	United States		11351	TWC-11351-NORTHEASTUS	true
2.36.64.159	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
198.2.51.242	unknown	United States		20001	TWC-20001-PACWESTUS	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
109.50.149.241	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
69.119.123.159	unknown	United States		6128	CABLE-NET-1US	true
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 17:55:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
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:	mal92.troj.evad.winMSI@10/11@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 81% • 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): dllhost.exe, VSSVC.exe, svchost.exe
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtFsControlFile calls found.
- Report size getting too big, too many NtOpenFile calls found.

- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- VT rate limit hit for: r3zg12.msi

Simulations

Behavior and APIs

Time	Type	Description
17:57:02	API Interceptor	1844x Sleep call for process: msiexec.exe modified
17:57:33	API Interceptor	23x Sleep call for process: rundll32.exe modified
17:57:33	API Interceptor	247x Sleep call for process: wscript.exe modified
17:57:37	API Interceptor	179x 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\725f14.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	8650
Entropy (8bit):	5.53533566252833
Encrypted:	false
SSDEEP:	96:ke6Ke2crqUNPw9CsAqWUNPw9C6jvogU/AqmHVP0cdxnG3ciuHsjfLwCUVp3B2BJB:kqeH9wgS9wgvcnY3UVpi
MD5:	C3EE277FD29FA58F348CE837640A6248
SHA1:	9A776BC167BD6816A2F16488D1CA279144076CE2
SHA-256:	5C577159B0F56A406D538702FC2E0E56F66E43CDF0E39C4BFB5F4681317B4A45
SHA-512:	51EE05D5D9CD3A78ACB82F44E746B33F0DD0E2E93AAF77AC0FA95C594D65A8E270F97A703FEE8236BD4C0F660C1B80364D14A0AF117D17C60FC4AB676B9E5F2
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%
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:\Users\user\AppData\Local\Temp\~DF737A82605D542653.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:\Users\user\AppData\Local\Temp\~DF9424631930F5E6F6.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:	....

C:\Users\user\AppData\Local\Temp\~DFCE21E83529306783.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.12150165085044722
Encrypted:	false
SSDEEP:	24:jIAWMQQt7E818lOdWmDqqrb9ipVIdWmDqqrb9ipV7VlwGklrkgV+rRH:cAWMNC818lEOMSoOMS5RrV
MD5:	152881F8DC204D99AEBA2705A3782FCB
SHA1:	660CC21C9CAC248ABAEDB2BA0C5584BCA6336755
SHA-256:	9BF23AB3B18670ADA93F47C692FADA5B6652AC14C1887F6D78932E237B141BE6
SHA-512:	DC0C2C8B8A2BAE9227538E8AECC236B9ED99E5BFFDC2E848B13303ECEE8215E20ECCE5764193847093708A90F8860AA96A5BD302228E83194706612C054D54E 9
Malicious:	false
Preview:	....

C:\Windows\Installer\725f12.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\725f13.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):	1.5290834806885116
Encrypted:	false
SSDEEP:	24:JoFC/lym6cpmUHCAjluSwPc+rVdWmDqqrb9ipV7VIwGklrkgsdWmDqqrb9ipVi8d:K0+cDHBluIEOMS5RrmOMSI818lnAWMN
MD5:	F79FA452955160DEA66B355C79633348
SHA1:	DF8591F44D592B2DED4CC19C50944D0C9C7A1EA2
SHA-256:	98D499E3EE487BC8A41B4339F34E48ADF45D504D743F381DBA3979CF4B63BA46
SHA-512:	663F75D95F9B059DDAC7AFFA125891EF193463A15B631B2E587E5DCF10D29EB770542080317BB493C75972C197B291A271EEB7E3CD8DE720135D24BB10D28A9
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\725f15.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, Nu mber 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:	D30110DC240790A1F0C15DF31069D361F80DF327C258DD3305E70EB9EE3814C285AB6290E88E4072B375F7DAC3D183D22ABA29CB94FDD7DB937C4399C18AD3 E
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSIDFB6.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	5.574222322102891
Encrypted:	false
SSDEEP:	48:VT5zj3JwCP3NDufgzYjRBoD8SY1eU/Fn9nhaEVlt+Xtu2:V/rYjrAueGnaEPi
MD5:	D677AFC93165EECE0A0BF927F0813BC0
SHA1:	374BAA5C81F013F5A665D23376BE78FD27A97A26
SHA-256:	9C430E95C05E227034C66BBFE82596D108E698689CE7146E1A64139674C29607
SHA-512:	27A88CACD02BB8AE072098411E8F52C22FC91FF0B6B2BECE3FED8910E531BF16BCFF408D63E062BA400D548893C2DBFEBAAA1B894248E149640047D535AC43 B8
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\725f12.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):	1.1629135735710199
Encrypted:	false
SSDEEP:	12:JSbX72FjRAGiLIlHVRpth/77777777777777777777777vDHFZRwpSl0i8Q:J3Ql5p0F
MD5:	43D53436CE3F850800B0ACC9CDAA39B9
SHA1:	E7C780CC0555D1E5A10AF2B0736C1985D2294758
SHA-256:	913C3DA22ABBA627ECFB121EF494CDC045D0BD6659BE7C8F2FD2328A45ED879C
SHA-512:	6D41E88A82F3515194869BCC7D66EE28E6A2FFF9B3861A5CC10D5A60F8175E61C20C34AB9C00F7978053C21803C6337FA6FCD156F4A4FB69183ED2155191613
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

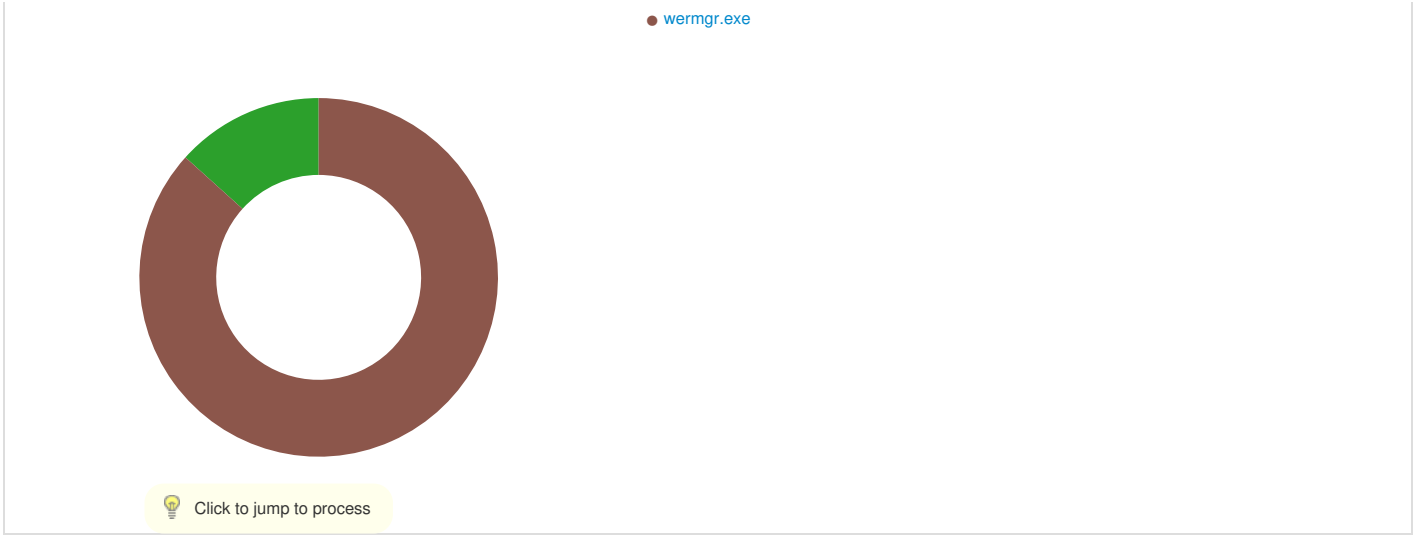
Network Behavior

No network behavior found

Statistics

Behavior

- msiexec.exe
- msiexec.exe
- rundll32.exe
- wscript.exe
- rundll32.exe



System Behavior

Analysis Process: msiexec.exe PID: 2364, Parent PID: 1860

General

Target ID:	1
Start time:	17:57:02
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:	0xff920000
File size:	128512 bytes
MD5 hash:	AC2E7152124CEED36846BD1B6592A00F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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: 2184, Parent PID: 404

General

Target ID:	2
Start time:	17:57:02
Start date:	30/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0xff920000
File size:	128512 bytes
MD5 hash:	AC2E7152124CEED36846BD1B6592A00F

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: rundll32.exe PID: **3244**, Parent PID: **2184**

General

Target ID:	5
Start time:	17:57:33
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:	0xff470000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
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	FF4727D0	ReadFile
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	264	success or wait	1	FF47281C	ReadFile

Analysis Process: wscript.exe PID: **3252**, Parent PID: **2184**

General

Target ID:	6
Start time:	17:57:33
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:	0xff120000
File size:	168960 bytes
MD5 hash:	045451FA238A75305CC26AC982472367
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 3260, Parent PID: 3244

General

Target ID:	7
Start time:	17:57:33
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:	0xf20000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000007.00000002.1071797162.000000000029D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000007.00000002.1072022431.0000000000E3D000.00000004.00000020.00020000.00000000.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: 3332, Parent PID: 3260

General

Target ID:	8
Start time:	17:57:36
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0xbd0000
File size:	53760 bytes
MD5 hash:	C9905EA4C326DAB778B9297BA5BD1889
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\Ovanpire	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	132CEB	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	13E746	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	success or wait	1	13AC70	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	ba1a3b32	binary	E6 B3 84 5E 06 3E B7 1B 23 63 9C 5C 66 E9 BB 09 28 C7 39 65 4B 30 96 BB 82 98 58 86 51 92 6D B4 06 68 4F 58 9D 5B 91 5E E4 C4 B4 6F 25 B6 C6 9C 32 6D	success or wait	1	13B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	8f85eb7c	binary	C3 01 D1 3C 89 AA A5 D2 79 54 DF 16 AD 90 3B 5D E3 82 77 53 E2 06 2A DA DF 00 19 60 0B 63 04 26 17 BF 53 46 06 13 5A 18 52 C5 38 CD FC 65 D8 C4 E6 62 30 19 09 8A 0E 93 E3 BA 92 49 FC E4 DF 08 08 84 3A 1E B9 CF 30 FD 88 D0 18 60 E1 82 A8 83 C8 29 01 EC A9 44 E7 27 B4 8B F5 CA 7E 6A C9 90 80 49 AA 03 14 41 FB B9 6B 0A 18 06 BC 32 6B 30 6A 56 53 43 8D 8B 19 B2 BA 27 D0 50 6B 3C 2E C9 83 62 59 63 1B D1 1C A2 87 70 E6 1D D3 3F EF 6A	success or wait	1	13B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	8dc4cb00	binary	40 9E 71 9F 60 2A EC 6F 25 47 3F 61 59 7E DB 2B ED AD 7E 9C 09 A5 5D 81 63 84 0B F3 41 94 12 08 49 63 D1 10 ED FF B4 9D E0 34 41 42 28 90 25 8C 10 A8 E3 63 00 85 E4 95 59 90 97 20 EA AA 86 7D 06 15 91 89 15 A9 9C 33 86 F9 50 22 61 42 CA 5F D3 20 05 E2 78 79 20 EC	success or wait	1	13B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	3578ac65	binary	54 68 2B AF F1 07 9E 0D F9 BE CC D5 BC 7F CF 94 1A F4 63 EF 85 C9 98	success or wait	1	13B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	4870e3ef	binary	4E 47 12 AB FB C1 42 14 CE 33 25 81 01 84 3B D1 8B 35 8E 9B 6D 5E 42 E9 C0 E2 52 9B E1 0B	success or wait	1	13B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	f0cc848a	binary	F6 85 8E 60 C3 88 AA 1E 6D 5C 57 37 7F 2B 9D 88 B0 50 8B 69 06 E4 84 29 1A 00 C7 0E F7 49 CB 20 B5 CA 2C 5B EF 90 FE 4A FD 3E 8E 0F 3D 7B 25 3B 63 23 EF FF DD AC 9E 9B	success or wait	1	13B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	37398c19	binary	63 46 5F B9 7D F6 F1 A4 93 BB 0B AB A6 5F 6A 9A 4F 90 45 F2 AC F1 B5 78 A9 A4 C8 92 C6 1B	success or wait	1	13B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	c55354c4	binary	B9 F8 5D 5C 32 21 23 CA 03 23 F1 55 A2 CE E6 14 7C 4D C5 58 A4 E8 56 1D 11 AE 47 C9 93 6C 33 78 62 86 15 1C 24 75 56 99 54 DA A2 B5 9C B2 69 B9 94 95 E3 67 DA CF F2 A3 9F 9A 46 59 CE DE 09 E3 70 65 30 3D 94 BD 63 5A DB 0D 1A 85 BD C5 C1 A0 CF 48 AE F1 0E 0E 9C EC B2 B0 98 F8 90 C5 F4 E6 E9 24 08 23 5C 1C 5D 4C F7 04 B0 76 4F 55 CB 49 5C 61	success or wait	1	13B195	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	ba1a3b32	binary	E6 B3 84 5E 06 3E B7 1B 23 63 9C 5C 66 E9 BB 09 28 C7 39 65 4B 30 96 BB 82 98 58 86 51 92 6D B4 06 68 4F 58 9D 5B 91 5E E4 C4 B4 6F 25 B6 C6 9C 32 6D	E6 B3 9F 5E 06 3E 86 D3 00 69 03 0A AE EA 2D DC CA 9A 35 E3 6E 46 F2 13 E5 20 0A 33 37 19 1B 56 EB BD DD 7C F4 3F 7E BB 37 DD 07 DC 17 31 18 F6 B2 87 74 D8 3F 58 11 B4 8C 49 E4 81 F4 7C B2 AF E2 C5 89 B1 43 20 8E 51 8B 3B EF	success or wait	1	13B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Vlotrabeib	ba1a3b32	binary	E6 B3 9F 5E 06 3E 86 D3 00 69 03 0A AE EA 2D DC CA 9A 35 E3 6E 46 F2 13 E5 20 0A 33 37 19 1B 56 EB BD DD 7C F4 3F 7E BB 37 DD 07 DC 17 31 18 F6 B2 87 74 D8 3F 58 11 B4 8C 49 E4 81 F4 7C B2 AF E2 C5 89 B1 43 20 8E 51 8B 3B EF	E6 B3 9F 5E 06 3E 86 D3 00 69 03 0A AE EA 2D DC CA 9A 35 E3 6E 46 F2 13 E5 20 0A 33 39 1F 15 56 EB BD DD 7C F4 3F 7E BB 37 DD 07 DC 17 31 18 F6 B2 87 74 D8 3F 58 11 B4 8C 49 E4 81 F4 7C B2 AF E2 C5 89 B1 43 20 8E 51 8B 3B EF	success or wait	1	13B195	RegSetValueExA

Disassembly

No disassembly