ID: 878630
Sample Name: 15dasx.msi
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:46:08
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report 15dasx.msi 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: Qbot 5
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
Hooking and other Techniques for Hiding and Protection 7
Anti Debugging 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
Public IPs 11
General Information 14
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Config.Msi\6bb81c.rbs 15
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll 15
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\notify.vbs 16
C:\Users\user\AppData\Local\Temp\~DF4899FDBF77CB7EDE.TMP 16
C:\Users\user\AppData\Local\Temp\~DFA9753353B6A77A75.TMP 16
C:\Users\user\AppData\Local\Temp\~DFC65A62CAF401C2CF.TMP 16
C:\Windows\Installer\6bb81a.msi 17
C:\Windows\Installer\6bb81b.ipi 17
C:\Windows\Installer\6bb81d.msi 17
C:\Windows\Installer\MSI8ED9.tmp 18
C:\Windows\Installer\SourceHash{64EDF889-FC17-466B-8E9A-5A8688EB1CDC} 18
Static File Info 18
General 18
File Icon 19
Network Behavior 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: msiexec.exePID: 2076, Parent PID: 1860 19
General 19

File Activities 20
Analysis Process: msiexec.exePID: 1188, Parent PID: 404 20
General 20
File Activities 20
Registry Activities 20
Analysis Process: rundll32.exePID: 2196, Parent PID: 1188 20
General 21
File Activities 21
File Read 21
Analysis Process: wscript.exePID: 1212, Parent PID: 1188 21
General 21
File Activities 21
Analysis Process: rundll32.exePID: 2120, Parent PID: 2196 21
General 21
File Activities 22
Analysis Process: wermgr.exePID: 2620, Parent PID: 2120 22
General 22
File Activities 22
File Created 22
File Read 22
Registry Activities 22
Key Created 22
Key Value Created 22
Key Value Modified 23
Disassembly 24

Windows Analysis Report

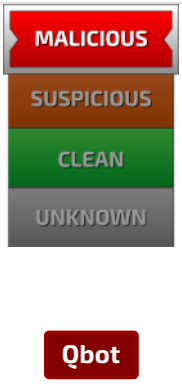
15dasx.msi

Overview

General Information

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

Detection



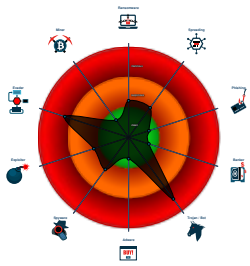
Qbot

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- msiexec.exe (PID: 2076 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\15dasx.msi" MD5: AC2E7152124CEED36846BD1B6592A00F)
- msiexec.exe (PID: 1188 cmdline: C:\Windows\system32\msiexec.exe /V MD5: AC2E7152124CEED36846BD1B6592A00F)
  - rundll32.exe (PID: 2196 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2120 cmdline: rundll32.exe C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll,next MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 2620 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: C9905EA4C326DAB778B9297BA5BD1889)
  - wscript.exe (PID: 1212 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": "BB30",
  "Campaign": "1685433861",
  "Version": "404.1320",
  "C2 list": [
    "12.172.173.82:50001",
    "178.175.187.254:443",
    "65.95.141.84:2222",
    "205.237.67.69:995",
    "83.110.223.61:443",
    "193.253.100.236:2222",
    "27.0.48.233:443",
    "102.159.188.125:443",
    "71.38.155.217:443",
    "58.186.75.42:443",
    "76.178.148.107:2222",
    "70.28.50.223:2087",
    "114.143.176.236:443",
    "51.14.29.227:2222",
    "59.28.84.65:443",
    "173.88.135.179:443",
    "103.144.201.56:2078",
    "96.87.28.170:2222",
    "105.186.128.181:995",
    "176.142.207.63:443",
    "151.62.238.176:443",
    "12.172.173.82:32101",
    "122.186.210.254:443",
    "82.125.44.236:2222",
    "84.108.200.161:443",
    "76.16.49.134:443",
    "70.28.50.223:32100",
    "12.172.173.82:465",
    "76.170.252.153:995",
    "184.182.66.109:443",
    "78.92.133.215:443",
    "50.68.204.71:993",
    "186.75.95.6:443",
    "113.11.92.30:443",
    "70.28.50.223:3389",
    "98.145.23.67:443",
    "85.57.212.13:3389",
    "50.68.186.195:443",
    "47.205.25.170:443",
    "12.172.173.82:993",
    "12.172.173.82:22",
    "69.242.31.249:443",
    "81.101.185.146:443",
    "79.168.224.165:2222",
    "75.143.236.149:443",
    "14.192.241.76:995",
    "86.195.14.72:2222",
    "81.229.117.95:2222",
    "220.240.164.182:443",
    "73.29.92.128:443",
    "12.172.173.82:21",
    "96.56.197.26:2222",
    "75.109.111.89:443",
    "76.86.31.59:443",
    "201.244.108.183:995",
    "68.203.69.96:443",
    "124.122.47.148:443",
    "122.184.143.86:443",
    "92.186.69.229:2222",
    "70.28.50.223:2083",
    "89.129.109.27:2222",
    "147.147.30.126:2222",
    "125.99.76.102:443",
    "88.126.94.4:50000",
    "151.65.167.77:443",
    "86.132.236.117:443",
    "92.154.17.149:2222",
    "223.166.13.95:995",
    "89.36.206.69:995",
    "96.56.197.26:2083",
    "78.18.105.11:443",
    "82.127.153.75:2222",
    "90.78.147.141:2222",
    "82.131.141.209:443",
    "183.87.163.165:443",
    "92.9.45.20:2222",
    "80.6.50.34:443",
    "80.12.88.148:2222",
    "69.133.162.35:443",
    "172.115.17.50:443",
    "95.45.50.93:2222",
    "12.172.173.82:2087",
    "103.140.174.20:2222"
```

```
      "103.140.174.20:2222",
      "24.198.114.130:995",
      "50.68.204.71:443",
      "69.119.123.159:2222",
      "64.121.161.102:443",
      "2.82.8.80:443",
      "184.181.75.148:443",
      "70.112.206.5:443",
      "198.2.51.242:993",
      "2.36.64.159:2078",
      "79.77.142.22:2222",
      "84.215.202.8:443",
      "147.219.4.194:443",
      "116.74.164.81:443",
      "70.28.50.223:2078",
      "12.172.173.82:995",
      "77.86.98.236:443",
      "104.35.24.154:443",
      "213.64.33.61:2222",
      "47.149.134.231:443",
      "72.134.124.16:443",
      "47.34.30.133:443",
      "103.42.86.42:995",
      "174.4.89.3:443",
      "161.142.103.187:995",
      "78.160.146.127:443",
      "84.35.26.14:995",
      "12.172.173.82:20",
      "70.28.50.223:2078",
      "124.149.143.189:2222",
      "70.160.67.203:443",
      "186.64.67.30:443",
      "103.123.223.133:443",
      "188.28.19.84:443",
      "174.58.146.57:443",
      "94.207.104.225:443",
      "86.97.55.89:2222",
      "69.123.4.221:2222"
    ]
  }
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.1050273322.00000000023DD000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000007.00000002.1050043697.000000000037D000.00000004.00000020.00020000.00000000.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.38a328.1.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
7.2.rundll32.exe.38a328.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
7.2.rundll32.exe.1b0000.0.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.1b0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
7.2.rundll32.exe.38a328.1.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

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

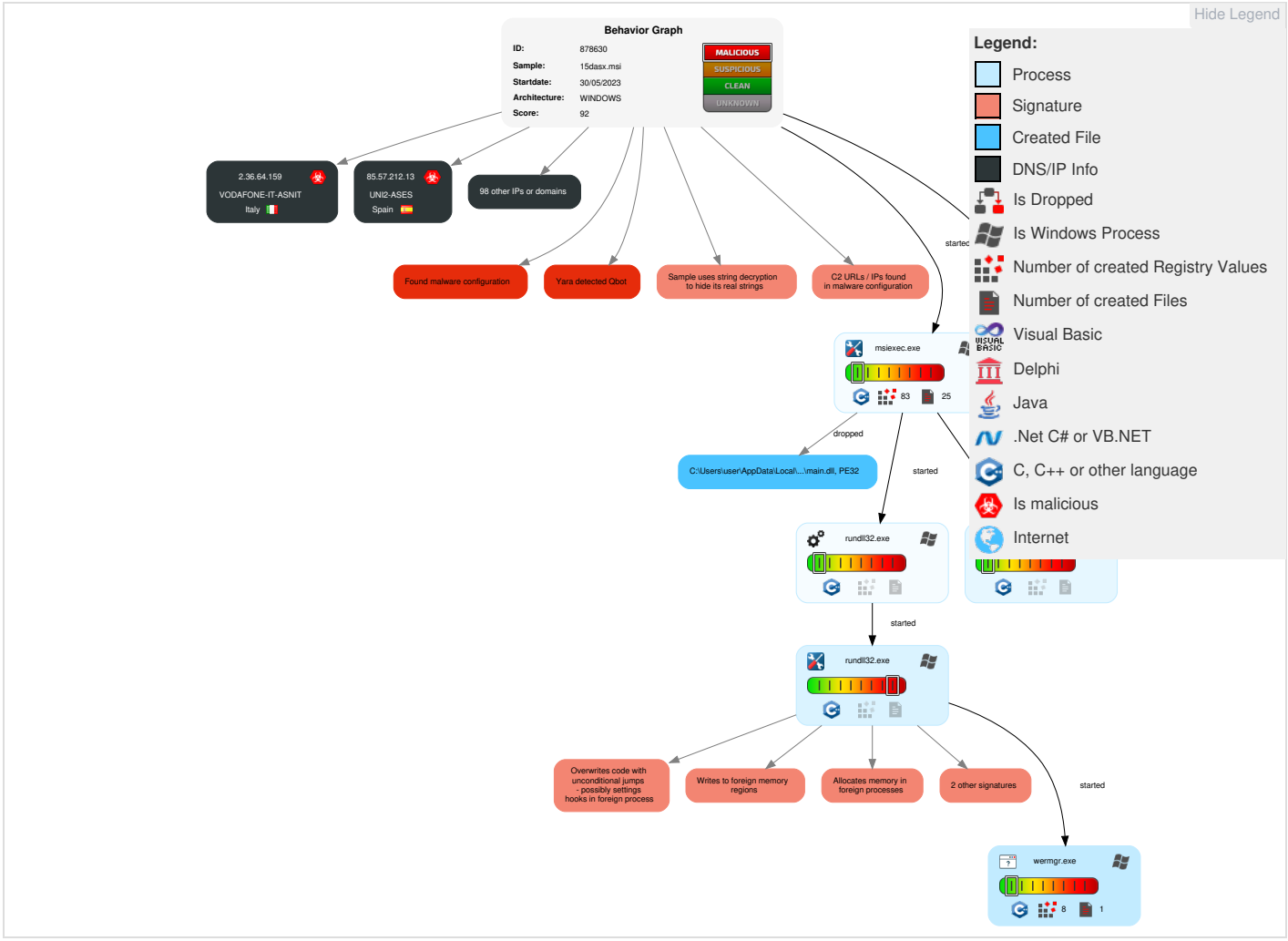
Yara detected Qbot

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	2 System Time Discovery	1 Replication Through Removable Media	1 Credential API Hooking	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	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 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 Peripheral Device Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Scripting	Cached Domain Credentials	2 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

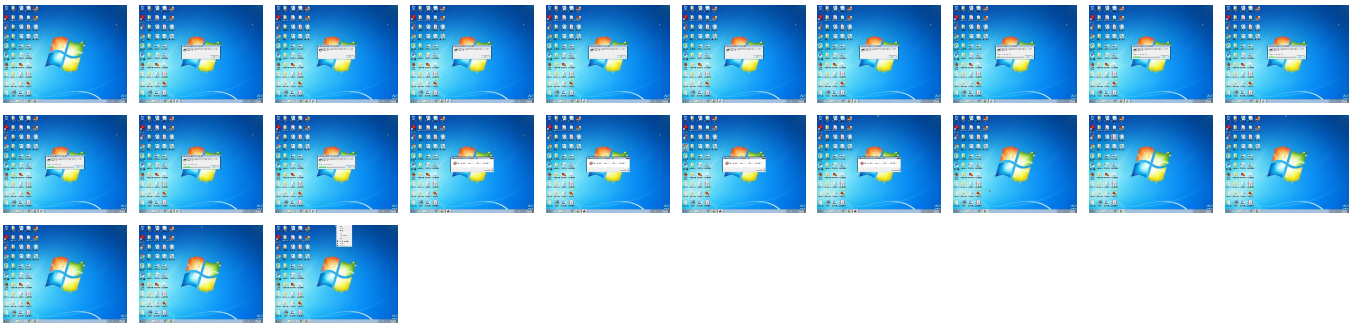
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
15dasx.msi	0%	ReversingLabs		

Dropped Files

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

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

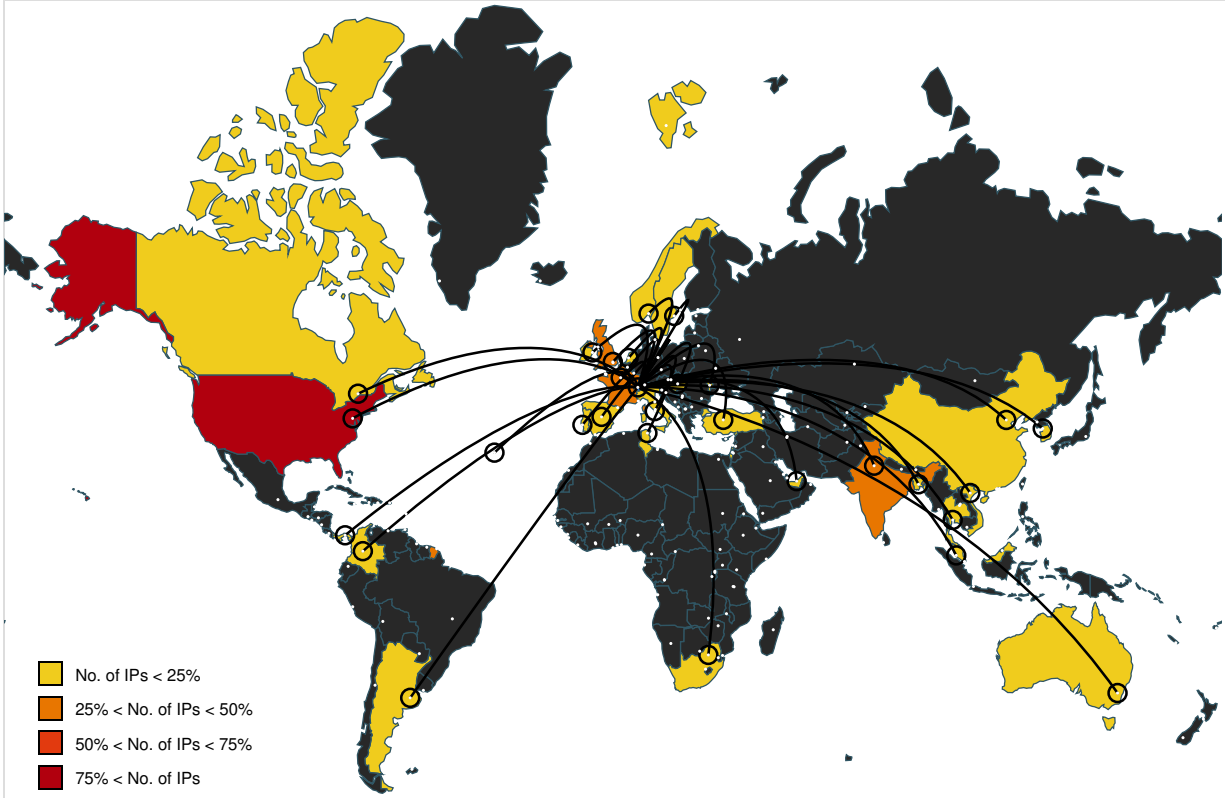
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://streams.videolan.org/upload/	rundll32.exe, rundll32.exe, 00000007.00000002.1050425390.00000000100AE000.00000002.00000001.01000000.00000006.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
75.143.236.149	unknown	United States		20115	CHARTER-20115US	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
86.195.14.72	unknown	France		3215	FranceTelecom-OrangeFR	true
84.215.202.8	unknown	Norway		41164	GET-NOGETNorwayNO	true
184.182.66.109	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
92.186.69.229	unknown	France		12479	UNI2-ASES	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
14.192.241.76	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
173.88.135.179	unknown	United States		10796	TWC-10796-MIDWESTUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.108.200.161	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	true
47.34.30.133	unknown	United States		20115	CHARTER-20115US	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
124.149.143.189	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
84.35.26.14	unknown	Netherlands		21221	INFOPACT-ASTheNetherlandsNL	true
73.29.92.128	unknown	United States		7922	COMCAST-7922US	true
68.203.69.96	unknown	United States		11427	TWC-11427-TEXASUS	true
82.131.141.209	unknown	Hungary		20845	DIGICABLEHU	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
178.175.187.254	unknown	Moldova Republic of		43289	TRABIAMD	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
186.64.67.30	unknown	Argentina		27953	NODOSUDSAAR	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
59.28.84.65	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
105.186.128.181	unknown	South Africa		37457	Telkom-InternetZA	true
76.86.31.59	unknown	United States		20001	TWC-20001-PACWESTUS	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
96.87.28.170	unknown	United States		7922	COMCAST-7922US	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
78.92.133.215	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
88.126.94.4	unknown	France		12322	PROXADFR	true
51.14.29.227	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
85.57.212.13	unknown	Spain		12479	UNI2-ASES	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
80.12.88.148	unknown	France		3215	FranceTelecom-OrangeFR	true
69.133.162.35	unknown	United States		11426	TWC-11426-CAROLINASUS	true
86.132.236.117	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
151.62.238.176	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
70.112.206.5	unknown	United States		11427	TWC-11427-TEXASUS	true
205.237.67.69	unknown	Canada		11290	CC-3272CA	true
102.159.188.125	unknown	Tunisia		37705	TOPNETTN	true
151.65.167.77	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
76.178.148.107	unknown	United States		10838	OCEANIC-INTERNET-RRUS	true
89.36.206.69	unknown	Italy		48544	TECNOADSL-ASIT	true
69.242.31.249	unknown	United States		7922	COMCAST-7922US	true
193.253.100.236	unknown	France		3215	FranceTelecom-OrangeFR	true
76.16.49.134	unknown	United States		7922	COMCAST-7922US	true
94.207.104.225	unknown	United Arab Emirates		15802	DU-AS1AE	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
78.18.105.11	unknown	Ireland		2110	AS-BTIREBTIrelandwaspreviouslyknownasEsatNetEUnet	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
103.144.201.56	unknown	unknown		139762	MSSOLUTION-AS-APSolutionBD	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
98.145.23.67	unknown	United States		20001	TWC-20001-PACWESTUS	true
47.149.134.231	unknown	United States		5650	FRONTIER-FRTRUS	true
82.125.44.236	unknown	France		3215	FranceTelecom-OrangeFR	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
89.129.109.27	unknown	Spain		12479	UNI2-ASES	true
122.186.210.254	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
90.78.147.141	unknown	France		3215	FranceTelecom-OrangeFR	true
122.184.143.86	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
213.64.33.61	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
86.97.55.89	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
78.160.146.127	unknown	Turkey		9121	TTNETTR	true
58.186.75.42	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
50.68.204.71	unknown	Canada		6327	SHAWCA	true
71.38.155.217	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
104.35.24.154	unknown	United States		20001	TWC-20001-PACWESTUS	true
220.240.164.182	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
24.198.114.130	unknown	United States		11351	TWC-11351-NORTHEASTUS	true
2.36.64.159	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
198.2.51.242	unknown	United States		20001	TWC-20001-PACWESTUS	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
69.119.123.159	unknown	United States		6128	CABLE-NET-1US	true
69.123.4.221	unknown	United States		6128	CABLE-NET-1US	true
172.115.17.50	unknown	United States		20001	TWC-20001-PACWESTUS	true
77.86.98.236	unknown	United Kingdom		12390	KINGSTON-UK-ASGB	true

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

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878630
Start date and time:	2023-05-30 22:46:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 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:	15dasx.msi
Detection:	MAL
Classification:	mal92.troj.evad.winMSI@10/11@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2.2% (good quality ratio 1.2%) • Quality average: 21.2% • Quality standard deviation: 26.1%
HCA Information:	• Successful, ratio: 94% • 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.

Simulations

Behavior and APIs

Time	Type	Description
22:46:58	API Interceptor	1641x Sleep call for process: msiexec.exe modified
22:47:25	API Interceptor	19x Sleep call for process: rundll32.exe modified
22:47:25	API Interceptor	224x Sleep call for process: wscript.exe modified
22:47:27	API Interceptor	184x 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\6bb81c.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	8650
Entropy (8bit):	5.55075152522519
Encrypted:	false
SSDEEP:	192:qXFAeUYEBwgq6YEBwg4rnNl0UVpK4XqaG/l:qW5wy5wFnj+
MD5:	2EB510D377D89068BE09E7B1E3D5A70A
SHA1:	DFF25995677E5F263F829188E8304ABDE3D994D5
SHA-256:	AE9951F7F09A03785CE94F7F4ECCD7A5DE0C4DE352234C83D6B6C929CBD03D04
SHA-512:	1DA3B55419CB12E97CF18639C794F15499284C534A59A9FFA5A5C2008E3BECEE3FA83CB08B54F72563497CB7A6D5B85A19B4377663E6C40145D6DB9C6FC1A1E5
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@..V.@.....@.....@.....@.....@.....@.....&.{64EDF889-FC17-466B-8E9A-5A8688EB1CDC}'.Adobe Acrobat PDF Browser Plugin 4.8.25..15dasx.msi .@.....@.....@.....@.....@.....&.{6ECD3C06-98A2-44A1-A41E-271C903F257F}.....@.....@.....@.....@.....@.....@.....@.....@....'.Adobe Acrobat PDF Browser Plugin 4.8.25..... .Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{82B5B2FD-2237-42AB-9F03-B3B9EAB30000}&.{64EDF889-FC17-466B-8E9A-5A8688EB1CDC}.@.....InstallFiles..Copying new files&.File: [1], Directory: [9], Size: [6]..:.C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\....B.C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll....D.C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\notify.vbs....WriteRegistryValues..Writing system registry values..Key: [1], Name: [2], Value: [3]$..@....%.Software\AdobeAcrobatPDFBrowserPlugin...@....(.&...AdobeAcrobatPDFBro

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

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	962048
Entropy (8bit):	6.7504689709982175
Encrypted:	false
SSDEEP:	24576:D7AkdHt+UnNtqbVotX4Dw/9JGCZdBK/+NYouXFPn/yd47:DZ8RDwlJGoY7X7
MD5:	A55C357391C089F93F5EF157BE209F63
SHA1:	A859A7AB02760EE8CD4DCF219EB1D460371350A8
SHA-256:	8D0C96718D4C7944FB648DF446D70ABBB87C5D4FF7C9735CF3BD9B2F11246A9E
SHA-512:	36152E39BACA8A0566C31DB97FF35D30E995FED246509C9816966D49F82143155225FE4BF07B7975DB1BEDC299008442FEC05D5A7588C18F6FD6EE1E821A471E

Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0d.....#...'.....0 .....{... ..@... .....hC.....0..x.....@..(A.....a.....(.....text...$.....`..`.data.....@....rda ta..$.....@..@.bss....d.....`.....edata..hC.....D...`.....@..@.idata.....@....CRT....0.....@....tls..... ..@....rsrc...N....0.....@....reloc..(A.....B...I.....@..B..... .....

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

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

C:\Users\user\AppData\Local\Temp\~DF4899FDBF77CB7EDE.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.06981092353499595
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOzTuC77BhXKPQVky6lS:2F0i8n0itFzDHFPuC77HWS
MD5:	82E43552F0F7875FD425564DAB1C45C5
SHA1:	A85775C63AF567CCBCEECF01E8E10B3CB56661E7
SHA-256:	31D5DF542C7533A468E811F5E32ABD1B0988FC35D56A233FFC4CA4211202FB2A
SHA-512:	F1936D8774A71CF61F23D07D5076864EE447765BCEF5C00C6647EF8951C6CABA1486ADAD3C986A2C6904567D6601CE5C49DF990772ACFD19B5A071779659284
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFA9753353B6A77A75.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.12120829877979931
Encrypted:	false
SSDEEP:	24:Cr7E818lOdWmDqqrb9ipVIdWmDqqrb9ipV7VIwGMlrkgQ+5:P818lEOMSoOMS5ZrQ
MD5:	F8B41D211697EEE05791DF7A862B3942
SHA1:	63B8F609BB546B14FBDB82E1B13B436A94260BBD
SHA-256:	55C89653912C2FE98C7DC855191898A4445FA78AE8C557CAABC00B58C5554747
SHA-512:	69247B964C815EAEAD5FDF960522BF3ADD008C9639A6C2B220F6A9CB8782393B7F4991FA71702BF2A7C3843FA03E3A0D4C8C34121B8D564B569E46AEEB6A075F
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFC65A62CAF401C2CF.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\Installer\6bb81a.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Adobe Acrobat PDF Browser Plugin 4.8.25, Author: Adobe Inc., Keywords: Installer, Comments: Adobe Acrobat PDF Browser Plugin, Template: Intel;1033, Revision Number: {6ECD3C06-98A2-44A1-A41E-271C903F257F}, Create Time/Date: Tue May 30 15:19:58 2023, Last Saved Time/Date: Tue May 30 15:19:58 2023, Number of Pages: 200, Number of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Category:	dropped
Size (bytes):	516096
Entropy (8bit):	7.918002678282303
Encrypted:	false
SSDEEP:	6144:jESkw7402pCiyBH6DIlxtWb9jOyHLmsjzcGet8Rghs0O892YptgrGzjkacDO+cDb:3kdiMHHLmKzQ8tfacDO+wVydjSavjQ
MD5:	AB8EF3423324168D06B2D122F75CA130
SHA1:	A7E273DDD7CDF303E366CBA16ABFD4C3966F2CF6
SHA-256:	4E70DA2D2EFC833EB5C450C9F82AAA7D433E31E39DC4EC36CA3C5DDDE0F4DC00
SHA-512:	8AADA720840A74A361D92DB1174D3AE8119FF2F70903A396BC0AE60ACFDFDF5D7FB781315B155F0B507B7B260A3F4FF8435DC9BA13E05F1547F2ABEA0C7DA220
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\6bb81b.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):	1.5277141372259355
Encrypted:	false
SSDEEP:	24:JnFC/lym6cpmUHCAjluSXG+PdWmDqqrb9ipV7VIwGMlrkgsdWmDqqrb9ipVi8183:x0+cDHBluFqOMS5ZrmOMSI818l
MD5:	4F184BE6D7D0C90A3675262A41E494CC
SHA1:	FF0A74C16271E7EEDF96732229B90492921B52EC
SHA-256:	72D06F2C743AE20C220767EAB4FEAF666CAF92E31D0EE37DD4253027FE2E2B3F
SHA-512:	01D6D55927575C2E494E1B6660573751279680392 9C0E1935325F638F8847B532F5399BF0F443416B34372060DA38A73F2AA0AED322F1A8048466F6E20578A4E
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\6bb81d.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Adobe Acrobat PDF Browser Plugin 4.8.25, Author: Adobe Inc., Keywords: Installer, Comments: Adobe Acrobat PDF Browser Plugin, Template: Intel;1033, Revision Number: {6ECD3C06-98A2-44A1-A41E-271C903F257F}, Create Time/Date: Tue May 30 15:19:58 2023, Last Saved Time/Date: Tue May 30 15:19:58 2023, Number of Pages: 200, Number of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Category:	dropped

Size (bytes):	516096
Entropy (8bit):	7.918002678282303
Encrypted:	false
SSDEEP:	6144:jESkw7402pCiyBH6DIlxtWb9jOyHLmsjzcGet8Rghs0O892YptgrGzjkacDO+cDb:3kdiMHHLmKzQ8tfacDO+wVydjSavjQ
MD5:	AB8EF3423324168D06B2D122F75CA130
SHA1:	A7E273DDD7CDF303E366CBA16ABFD4C3966F2CF6
SHA-256:	4E70DA2D2EFC833EB5C450C9F82AAA7D433E31E39DC4EC36CA3C5DDDE0F4DC00
SHA-512:	8AADA720840A74A361D92DB1174D3AE8119FF2F70903A396BC0AE60ACFDFDF5D7FB781315B155F0B507B7B260A3F4FF8435DC9BA13E05F1547F2ABEA0C7DA220
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\MSI8ED9.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	5.589708162392856
Encrypted:	false
SSDEEP:	48:vf1InOLJwCP3hDufg6YPRBoD8SY1eU/SnI1InCpfaEVltdtu1InMn:vXS+YPrAuedIofaEP8Mn
MD5:	98D6FE23EEFA66343D02362715DE6A1B
SHA1:	8F0C0BE4E71FF7D71A5A77DD823D70C39E506856
SHA-256:	65A632BED627509E9FF49A6A16666B11E4EBEA3A26FC069E6C156290F4023B0D
SHA-512:	F93FF717188D72156B2B1800427DBAC1445B045B2422859B9BFA160466AE6B9131595CCCB2826E99D850DC3D49A61BE0BF96478BE044EF693A641BE4B010190A
Malicious:	false
Preview:	...@IXOS.@.....@..V.@.....@.....@.....@.....@.....@.....&.{64EDF889-FC17-466B-8E9A-5A8688EB1CDC}'.Adobe Acrobat PDF Browser Plugin 4.8.25..15dasx.msi .@.....@.....@.....@.....@.....&.{6ECD3C06-98A2-44A1-A41E-271C903F257F}.....@.....@.....@.....@.....@.....@.....@.....@....'.Adobe Acrobat PDF Browser Plugin 4.8.25..... .Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@.....@. ....@.]....&.{82B5B2FD-2237-42AB-9F03-B3B9EAB30000}F.01:\Software\AdobeAcrobatPDFBrowserPlugin\AdobeAcrobatPDFBrowserPlugin.@.....@.....@.....@..... ...InstallFiles..Copying new files&.File: [1], Directory: [9], Size: [6]...@.....@.....@.....:.C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\..).1\xssanpen\ |AdobeAcrobatPDFBrowserPlugin\.....Please insert the disk: ..media3.cab.@.....@.....C:\Windows\Installer\6bb81a.msi.....@.....main.dll..dll_main..main.dll.@..... @.....@.....@...

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

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1628561562250028
Encrypted:	false
SSDEEP:	12:JSbX72Fj3SAGiLIlHVRpth/77777777777777777777777vDHFPuC77HrpSl0G:JUQI5pFBHlF
MD5:	A30D6EE443F5F383CD600F105CD74165
SHA1:	E5CCC5ADD0A5AB95D5168E4889C4D8BA6CB24CA5
SHA-256:	A1A5E17B1DDA584A2FBDF8AAB33A2F3962F8775A13E7E314CA344E04B4C5BDA7
SHA-512:	38F505EB2F6A414216EE88C79ED62CF6460C38564108BEAB177F8218A2E0262B4299D87DA52C1DFFC377C177FC94B08088187705 67DB211FB84AD90620A759A5
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: {6ECD3 C06-98A2-44A1-A41E-271C903F257F}, Create Time/Date: Tue May 30 15:19:58 2023, Last Saved Time/Date: Tue May 30 15:19:58 2023, Number of Pages: 200, Nu mber of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Entropy (8bit):	7.918002678282303

TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	15dasx.msi
File size:	516096
MD5:	ab8ef3423324168d06b2d122f75ca130
SHA1:	a7e273ddd7cdf303e366cba16abfd4c3966f2cf6
SHA256:	4e70da2d2efc833eb5c450c9f82aaa7d433e31e39dc4ec36ca3c5ddde0f4dc00
SHA512:	8aada720840a74a361d92db1174d3ae8119ff2f70903a396bc0ae60acfdfdf5d7fb781315b155f0b507b7b260a3f4ff8435dc9ba13e05f1547f2abea0c7da220
SSDEEP:	6144:jESkw7402pCiyBH6DllxtWb9jOyHLmsjzcGet8Rghs0O892YptgrGzjkacDO+cDb:3kdiMHHLmKzQ8tfacDO+wVydjSavjQ
TLSH:	DDB4231536022373C5014B72DC9D87ECA70A3E59756AB61F7E09F8480EB6B7D12B72A3
File Content Preview:	.....>.....

File Icon

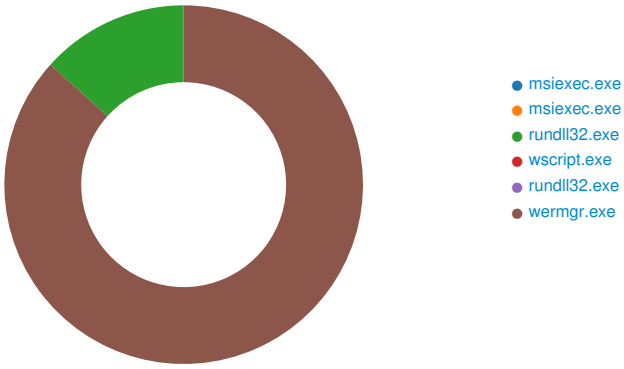
Icon Hash:	2d2e3797b32b2b99

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 2076, Parent PID: 1860

General	
Target ID:	1
Start time:	22:46:57
Start date:	30/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\15dasx.msi"

Imagebase:	0xff740000
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: **1188**, Parent PID: **404**

General

Target ID:	2
Start time:	22:46:58
Start date:	30/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0xff740000
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: **2196**, Parent PID: **1188**

General	
Target ID:	5
Start time:	22:47:25
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:	0xffa30000
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	FFA327D0	ReadFile
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	264	success or wait	1	FFA3281C	ReadFile

Analysis Process: wscript.exe PID: **1212**, Parent PID: **1188**

General	
Target ID:	6
Start time:	22:47:25
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:	0xff870000
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: **2120**, Parent PID: **2196**

General	
Target ID:	7
Start time:	22:47:25
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:	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: 00000007.00000002.1050273322.00000000023DD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000007.00000002.1050043697.000000000037D000.00000004.00000020.00020000.00000000.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: 2620, Parent PID: 2120

General

Target ID:	8
Start time:	22:47:27
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x2d0000
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\Xoauzizye	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	102CEB	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AdobeAcrobatPDFBrowserPlugin\main.dll	unknown	962048	success or wait	2	10E746	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	success or wait	1	10AC70	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	3f516fd7	binary	DB A7 A2 7D C6 32 1D CD 63 91 D4 1B BC A6 BD 18 2D 44 B8 47 C5 7C 6F B9 E7 FA 0E 61 72 AC 34 0A 80 71 50 5F 0C 59 32 5E 2D 5B 15 A8 07 C6 CF 6E A3 09 B0 8B CC CA BE EC 0E	success or wait	1	10B195	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	acebf99	binary	A6 B2 DB A9 7E CB 48 8A C0 DA 55 A8 C0 C5 02 BE 73 64 B8 66 3E 00 73 B5 72 93 9A 70 69 2E 71 58 0D 47 32 EF 53 BC AB 46 D7 47 18 88 12 21 F5 5D A2 DE F4 94 0F 97 20 35 47 F6 C1 C0 A5 A8 B2 4A 13 E9 A9 02 F0 EE 92 28 41 33 71 65 08 89 13 97 5E 7B D4 98 1C 65 CB A4 E5 57 DD 3D 7F D4 16 6E BF 8A FA FC E0 3B 43 4D 08 79 CC 01 FD 8A E7 44 EB 5D 86 AF 69 0D C3 4E 55 6B 27 A2 AF 8F 0E C3 59 79 CE 82 F2 98 D5	success or wait	1	10B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	88f9fe5	binary	55 69 4E 48 FB DE 91 EF DC A2 3D D4 6A 69 D1 F8 DE FE 1A BC 26 FD 3C AB C1 24 32 81 F6 CE 15 98 76 C2 6B 2D 5E DC 0F 86 9D 5C 02 1D 97 77 9E B6 7E AB 48 EB 87 E5 1A 48 BB 05 1A 19 D9 A7 CD 98 2C 22 48 FA 82 F0 93 3E 4C D2 F5 50 AF 8C 70 C5 A2 72 D7 EC B5 F1 EE 17 45 62 CD 28 D7 88 30 FE F0 57 7D 08 1A 7B 52 51 72 C8	success or wait	1	10B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	b033f880	binary	DD D7 60 C0 3E A0 1C 18 72 FE D6 4C A5 AB 36 11 0F AD FF 3A 26 17 1D 5D DC 6E D5 4C 61 36 55 BC 9F 3A 6E 8F 25 92 38 DC D1 9B 76 D8 ED 78 9B C2 9A 7F 75 E5 23 C6 AE C1 71 F1 3B 69 24 8E A9 6C D0 26 2B CA 02 3C 49 25 0E	success or wait	1	10B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	cd3bb70a	binary	B5 EC B0 7A 36 8B 28 8D FF CC 98 64 C2 32 84 18 D1 59 49 B4 68 E0 A8 11 69 9E 83 2C 90 0F AA 09 E0 B7 93 72 D3 30 6A 02 07 2B 7B BC 72 D9 95 36 CF 34 FD B6 C3 2A 8D 96 B4 A0 DA BE 65 9C A8 6C 99 78 87 61 CB A8 C9 6D B5 44 61 45 4E 7E 9A 5D 50 B7 13 2F C2 E7 3F 42 80 D2 A9 66 8D 27 2C 56 70 8C 4E 08 D7 55 50 24 11	success or wait	1	10B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	7587d06f	binary	B9 13 D0 5E B5 3E 44 C3 CF A0 63 98 09 8C 0C 17 5A F4 85 39 1E 64 38 F3 32 D3 BA 12 B1 FB DC 2F 38 22 F7 BF 2A 11 E2 80 E4 36 A9 CE EF A7 A6 72 2B 0C F3 29 00 D9 90 6E 77 07 97 DC 81 76 FD B4 B2 00 AA 9C 26 44 D3 F2 14 F9 24 E2 AC	success or wait	1	10B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	b272d8fc	binary	FC 49 75 9E AF 8F DA F2 4A 0B 03 C8 A0 83 77 D1 A1 65 23 3C 75 6D 69 7F 1E E6 20 81 6F 2B 29 7D 9C 79 15 D6 4B A5 B5 B2 23 82 63 E8 9B CC 06 E6 C4 5C 85 2A 25 25 7C 91	success or wait	1	10B195	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	40180021	binary	23 FF F3 36 5E 59 E7 69 4A E2 A2 8C 96 33 1F 0C B8 46 45 80 33 57 7D 05 03 2E 8D C1 76 F6 1F 56 E5 A0 38 7C 13 C4 97 E7 B1 52 C0 10 1B 84 F9 25 D2 B8 AC 3D 3B 1E 7F EA 4B 75 33 C3 9A C5 7D 45 BD 4F DB 7D 19 20 22 C6 0F 84 62 96 88 D7 FD C9 37 B0 5E 17 20 4A 67 B5 31 7B 2E 51 A4 E9 F5 72 54 B1 ED 53 89 80 53 D0 9A	success or wait	1	10B195	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	3f516fd7	binary	DB A7 A2 7D C6 32 1D CD 63 91 D4 1B BC A6 BD 18 2D 44 B8 47 C5 7C 6F B9 E7 FA 0E 61 72 AC 34 0A 80 71 50 5F 0C 59 32 5E 2D 5B 15 A8 07 C6 CF 6E A3 09 B0 8B CC CA BE EC 0E	DB A7 B9 7D C6 32 2C 9E 78 96 FC 59 6B 7A F3 14 C4 D3 07 0B 33 43 85 69 48 BA D2 C0 FC D1 F4 E1 63 7C 28 44 02 68 69 40 0A BC 1C 3C F1 7E 22 D9 0D 3C C3 6D 12 46 53 41 14 7D 41 71 9E A8 4E 50 33 4E 4B 31 02 3D BD 9B 60 E6 49 BC 6E 4A 68 DC E2 BB	success or wait	1	10B195	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\lprjuqt	3f516fd7	binary	DB A7 B9 7D C6 32 2C 9E 78 96 FC 59 6B 7A F3 14 C4 D3 07 0B 33 43 85 69 48 BA D2 C0 FC D1 F4 E1 63 7C 28 44 02 68 69 40 0A BC 1C 3C F1 7E 22 D9 0D 3C C3 6D 12 46 53 41 14 7D 41 71 9E A8 4E 50 33 4E 4B 31 02 3D BD 9B 60 E6 49 BC 6E 4A 68 DC E2 BB	DB A7 B9 7D C6 32 2C 9E 78 96 FC 59 6B 7A F3 14 C4 D3 07 0B 33 43 85 69 48 BA D2 C0 FE D6 F3 E1 63 7C 28 44 02 68 69 40 0A BC 1C 3C F1 7E 22 D9 0D 3C C3 6D 12 46 53 41 14 7D 41 71 9E A8 4E 50 33 4E 4B 31 02 3D BD 9B 60 E6 49 BC 6E 4A 68 DC E2 BB	success or wait	1	10B195	RegSetValueExA

Disassembly

No disassembly