ID: 437123
Sample Name: boI88C399w.exe
Cookbook: default.jbs
Time: 12:34:09
Date: 19/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

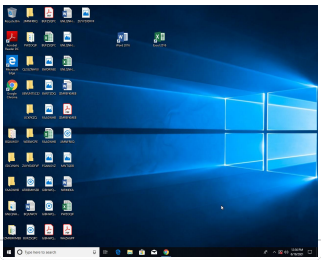
Windows Analysis Report boI88C399w.exe

Overview

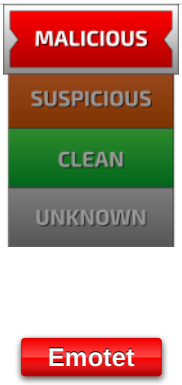
General Information

Sample Name:	boI88C399w.exe
Analysis ID:	437123
MD5:	0a82064af051bad.
SHA1:	f7bf190091d5fe3…
SHA256:	8f165a26d7e9ad7.
Infos:	

Most interesting Screenshot:



Detection



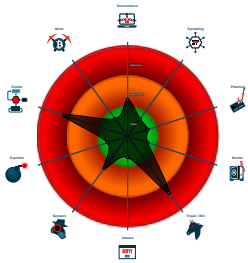
Emotet

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- C2 URLs / IPs found in malware con…
- Drops executables to the windows d…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Connects to several IPs in different …
- Contains capabilities to detect virtua…
- Contains functionality to call native f…
- Contains functionality to enumerate …

Classification



Process Tree

- **System is w10x64**
- boI88C399w.exe (PID: 7052 cmdline: 'C:\Users\user\Desktop\boI88C399w.exe' MD5: 0A82064AF051BAD014B77038D60474B6)
  - splwow64.exe (PID: 7072 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
  - KBDHU1.exe (PID: 4780 cmdline: C:\Windows\SysWOW64\mos\KBDHU1.exe MD5: 0A82064AF051BAD014B77038D60474B6)
- svchost.exe (PID: 7108 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6812 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7032 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5932 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhANQOcBKvh5xEW7VcJ9totsjdBwuAclxS\nQ0e09fk8V053lktpW3TRrzAW63yt6j1KWnyxMrU3igFXypBoI4lVNmkje4UPtIIS\nfkzjEIvG1v/ZNn1k0J0PfFTxbFFeUEs3AwIDAQAB",
  "C2 list": [
    "88.153.35.32:80",
    "107.170.146.252:8080",
    "173.212.214.235:7080",
    "167.114.153.111:8080",
    "202.141.243.254:443",
    "75.143.247.51:80",
    "85.105.111.166:80",
    "216.139.123.119:80",
    "113.61.66.94:80",
    "162.241.140.129:8080",
    "190.12.119.180:443",
    "2.58.16.89:8080",
    "91.211.88.52:7080",
    "93.147.212.206:80",
    "71.15.245.148:8080",
    "157.245.99.39:8080",
    "27.114.9.93:80",
    "50.91.114.38:80",
    "174.106.122.139:80",
    "47.36.140.164:80",
    "139.162.60.124:8080",
    "209.54.13.14:80",
    "217.20.166.178:7080",
```

```
"185.94.252.104:443",
"72.186.136.247:443",
"172.86.188.251:8080",
"41.185.28.84:8080",
"87.106.139.101:8080",
"89.216.122.92:80",
"108.46.29.236:80",
"184.180.181.202:80",
"173.63.222.65:80",
"120.150.60.189:80",
"62.30.7.67:443",
"139.99.158.11:443",
"220.245.198.194:80",
"138.68.87.218:443",
"201.241.127.190:80",
"186.74.215.34:80",
"190.162.215.233:80",
"24.178.90.49:80",
"89.121.205.18:80",
"5.39.91.110:7080",
"59.125.219.109:443",
"182.208.30.18:443",
"123.176.25.234:80",
"24.137.76.62:80",
"74.208.45.104:8080",
"194.187.133.160:443",
"37.179.204.33:80",
"194.4.58.192:7080",
"95.9.5.93:80",
"67.170.250.203:443",
"61.33.119.226:443",
"96.245.227.43:80",
"68.115.186.26:80",
"190.108.228.27:443",
"112.185.64.233:80",
"176.111.60.55:8080",
"91.146.156.228:80",
"190.240.194.77:443",
"115.94.207.99:443",
"62.171.142.179:8080",
"134.209.144.106:443",
"168.235.67.138:7080",
"124.41.215.226:80",
"172.104.97.173:8080",
"202.134.4.216:8080",
"94.200.114.161:80",
"67.163.161.107:80",
"61.76.222.210:80",
"97.82.79.83:80",
"74.214.230.200:80",
"46.105.131.79:8080",
"78.188.106.53:443",
"186.70.56.94:443",
"120.150.218.241:443",
"50.245.107.73:443",
"123.142.37.166:80",
"110.145.77.103:80",
"61.19.246.238:443",
"218.147.193.146:80",
"94.230.70.6:80",
"154.91.33.137:443",
"104.131.11.150:443",
"95.213.236.64:8080",
"49.50.209.131:80",
"187.161.206.24:80",
"37.139.21.175:8080",
"121.124.124.40:7080",
"200.116.145.225:443",
"24.230.141.169:80",
"194.190.67.75:80",
"209.141.54.221:7080",
"137.59.187.107:8080",
"217.123.207.149:80",
"24.133.106.23:80",
"79.137.83.50:443",
"24.179.13.119:80",
"202.134.4.211:8080",
"78.24.219.147:8080",
"76.175.162.101:80",
"121.7.31.214:80",
"62.75.141.82:80",
"109.74.5.95:8080",
"75.188.96.231:80",
"176.113.52.6:443",
"50.35.17.13:80",
"118.83.154.64:443",
"110.142.236.207:80",
"188.219.31.12:80",
"72.143.73.234:443",
"102.182.93.220:80",
"66.76.12.94:8080"
```

```
      "103.86.49.11:8080",
      "190.164.104.62:80",
      "203.153.216.189:7080",
      "119.59.116.21:8080",
      "172.105.13.66:443",
      "94.23.237.171:443",
      "49.3.224.99:8080",
      "139.59.60.244:8080",
      "172.91.208.86:80"
    ]
  }
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.663798235.0000000002CC1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000003.716674491.00000000032E2000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.906181296.0000000002341000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000003.658508716.0000000000602000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.906600906.00000000032D0000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.boI88C399w.exe.62a3d0.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.boI88C399w.exe.62a3d0.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.boI88C399w.exe.2cc0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.3.KBDHU1.exe.32e32a0.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.boI88C399w.exe.62a3d0.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Emotet

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

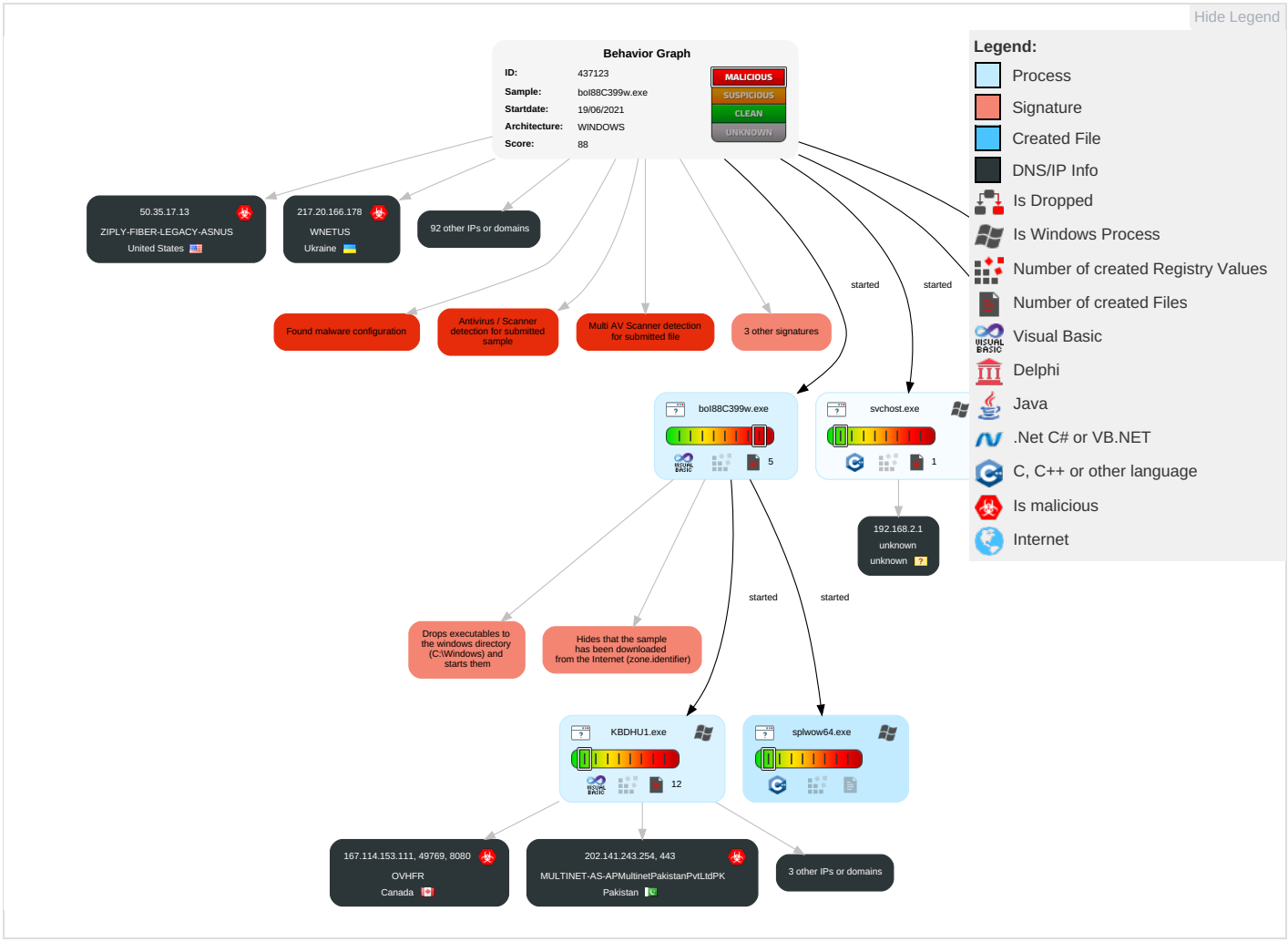
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Eff
Valid Accounts	Service Execution 1	Windows Service 2	Windows Service 2	Masquerading 1 2	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 2	Eav Inse Net Cor
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 2	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exp Rec Cal
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exp Tra Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mai Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jan Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	System Service Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	File and Directory Discovery 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Information Discovery 1 5	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols	

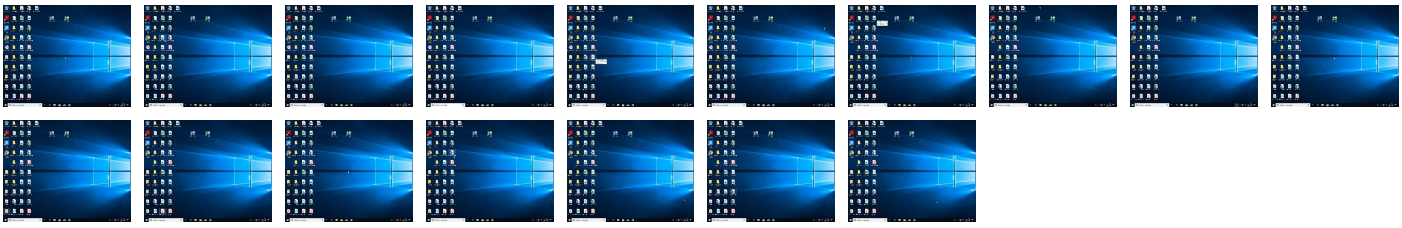
Behavior Graph



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
bol88C399w.exe	82%	Virustotal		Browse
bol88C399w.exe	71%	Metadefender		Browse
bol88C399w.exe	90%	ReversingLabs	Win32.Trojan.Emotet	
bol88C399w.exe	100%	Avira	TR/AD.Emotet.fkb	
bol88C399w.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.bol88C399w.exe.62a3d0.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.bol88C399w.exe.62a3d0.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.bol88C399w.exe.2cc0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.3.KBDHU1.exe.32e32a0.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.KBDHU1.exe.2340000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.KBDHU1.exe.32e32a0.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://173.212.214.235:7080/hO5dkT/0EDa/Mr7phtrE381/twO6hvq/FJxtI0//	0%	Avira URL Cloud	safe	
http://88.153.35.32/jGQKlmkSoBBnbOFUuBG/9vXEjmEP4GznF/&	0%	Avira URL Cloud	safe	
http://202.141.243.254:443/ZTcUlmgOk/ZdXDncN6R/750%	0%	Avira URL Cloud	safe	
http://202.141.243.254:443/ZTcUlmgOk/ZdXDncN6R/x	0%	Avira URL Cloud	safe	
http://75.143.247.51/8252jRzGZ1ESaMRhm/ZvhIlyMvd/AluncWtMpTGrO/1f9mgY7KN8T/YXKrl/nDV3S4P6PnM/s	0%	Avira URL Cloud	safe	
http://75.143.247.51/8252jRzGZ1ESaMRhm/ZvhIlyMvd/AluncWtMpTGrO/1f9mgY7KN8T/YXKrl/nDV3S4P6PnM/v5s%	0%	Avira URL Cloud	safe	
http://167.114.153.111:8080/K5ZJo5zQ/HcfJcbQPbzw55g8/vSjTj/8XztFu/4uKa0U6RLsViXlFaMpW/6	0%	Avira URL Cloud	safe	
http://167.114.153.111:8080/K5ZJo5zQ/HcfJcbQPbzw55g8/vSjTj/8XztFu/4uKa0U6RLsViXlFaMpW/v	0%	Avira URL Cloud	safe	
http://173.212.214.235:7080/hO5dkT/0EDa/Mr7phtrE381/twO6hvq/FJxtI0//tItqVujt/djBiHrQbZlsTCQpMosu/bqx	0%	Avira URL Cloud	safe	
http://167.114.153.111:8080/K5ZJo5zQ/HcfJcbQPbzw55g8/vSjTj/8XztFu/4uKa0U6RLsViXlFaMpW/K	0%	Avira URL Cloud	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://167.114.153.111:8080/K5ZJo5zQ/HcfJcbQPbzw55g8/vSjTj/8XztFu/4uKa0U6RLsViXlFaMpW/	0%	Avira URL Cloud	safe	
http://107.170.146.252:8080/yYXdTFdZ0/DfPFFYTbrJqLTvn/OUI1VCQMV00VFH/tItqVujt/djBiHrQbZlsTCQpMosu/bq	0%	Avira URL Cloud	safe	
http://88.153.35.32/jGQKlmkSoBBnbOFUuBG/9vXEjmEP4GznF/	0%	Avira URL Cloud	safe	
http://75.143.247.51/8252jRzGZ1ESaMRhm/ZvhIlyMvd/AluncWtMpTGrO/1f9mgY7KN8T/YXKrl/nDV3S4P6PnM/V	0%	Avira URL Cloud	safe	
http://173.212.214.235:7080/hO5dkT/0EDa/Mr7phtrE381/twO6hvq/FJxtI0/A:	0%	Avira URL Cloud	safe	
http://202.141.243.254:443/ZTcUlmgOk/ZdXDncN6R/)5Z%	0%	Avira URL Cloud	safe	
http://75.143.247.51/8252jRzGZ1ESaMRhm/ZvhIlyMvd/AluncWtMpTGrO/1f9mgY7KN8T/YXKrl/nDV3S4P6PnM/R	0%	Avira URL Cloud	safe	
http://75.143.247.51/8252jRzGZ1ESaMRhm/ZvhIlyMvd/AluncWtMpTGrO/1f9mgY7KN8T/YXKrl/nDV3S4P6PnM/	0%	Avira URL Cloud	safe	
http://202.141.243.254:443/ZTcUlmgOk/ZdXDncN6R/	0%	Avira URL Cloud	safe	
http://75.143.247.51/8252jRzGZ1ESaMRhm/ZvhIlyMvd/AluncWtMpTGrO/1f9mgY7KN8T/YXKrl/nDV3S4P6PnM/Q	0%	Avira URL Cloud	safe	
http://173.212.214.235:7080/hO5dkT/0EDa/Mr7phtrE381/twO6hvq/FJxtI0/	0%	Avira URL Cloud	safe	
http://167.114.153.111:8080/K5ZJo5zQ/HcfJcbQPbzw55g8/vSjTj/8XztFu/4uKa0U6RLsViXlFaMpW//	0%	Avira URL Cloud	safe	
http://75.143.247.51/8252jRzGZ1ESaMRhm/ZvhIlyMvd/AluncWtMpTGrO/1f9mgY7KN8T/YXKrl/nDV3S4P6PnM/)	0%	Avira URL Cloud	safe	
http://167.114.153.111:8080/K5ZJo5zQ/HcfJcbQPbzw55g8/vSjTj/8XztFu/4uKa0U6RLsViXlFaMpW/(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.4.58.192	unknown	Kazakhstan		202958	HOSTER-KZ	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
102.182.93.220	unknown	South Africa		37611	AfrihostZA	true
95.9.5.93	unknown	Turkey		9121	TTNETTR	true
94.200.114.161	unknown	United Arab Emirates		15802	DU-AS1AE	true
72.186.136.247	unknown	United States		33363	BHN-33363US	true
115.94.207.99	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
89.121.205.18	unknown	Romania		9050	RTDBucharestRomaniaRO	true
24.133.106.23	unknown	Turkey		47524	TURKSAT-ASTR	true
216.139.123.119	unknown	United States		395582	GRM-NETWORKUS	true
200.116.145.225	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
138.68.87.218	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.13.66	unknown	United States		63949	LINODE-APLinodeLLCUS	true
220.245.198.194	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
67.170.250.203	unknown	United States		7922	COMCAST-7922US	true
104.131.11.150	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
176.111.60.55	unknown	Ukraine		24703	UN-UKRAINE-ASKievUkraineUA	true
24.178.90.49	unknown	United States		20115	CHARTER-20115US	true
94.23.237.171	unknown	France		16276	OVHFR	true
187.161.206.24	unknown	Mexico		11888	TelevisionInternacionalSAdeCVMX	true
41.185.28.84	unknown	South Africa		36943	GridhostZA	true
194.190.67.75	unknown	Russian Federation		50804	BESTLINE-NET-PROTVINORU	true
186.74.215.34	unknown	Panama		11556	CableWirelessPanamaPA	true
202.134.4.216	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
120.150.218.241	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
202.134.4.211	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
87.106.139.101	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
62.30.7.67	unknown	United Kingdom		5089	NTLGB	true
123.142.37.166	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
75.143.247.51	unknown	United States		20115	CHARTER-20115US	true
49.3.224.99	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	true
162.241.140.129	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
124.41.215.226	unknown	Nepal		17501	WLINK-NEPAL-AS-APWorldLinkCommunicationsPvtLtdNP	true
62.75.141.82	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
119.59.116.21	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
113.61.66.94	unknown	Australia		45510	TELCOINABOX-AULevel109HunterStreetAU	true
96.245.227.43	unknown	United States		701	UUNETUS	true
172.91.208.86	unknown	United States		20001	TWC-20001-PACWESTUS	true
37.139.21.175	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
194.187.133.160	unknown	Bulgaria		13124	IBGCBG	true
121.7.31.214	unknown	Singapore		9506	SINGTEL-FIBRESingtelFibreBroadbandSG	true
112.185.64.233	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
61.76.222.210	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
95.213.236.64	unknown	Russian Federation		49505	SELECTELRU	true
46.105.131.79	unknown	France		16276	OVHFR	true
27.114.9.93	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
74.214.230.200	unknown	United States		36728	EMERYTELCOMUS	true
190.162.215.233	unknown	Chile		22047	VTRBANDAANCHASACL	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
110.145.77.103	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
120.150.60.189	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
154.91.33.137	unknown	Seychelles		137443	ANCHGLOBAL-AS-APAnchnetAsiaLimitedHK	true
107.170.146.252	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.147.212.206	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
91.211.88.52	unknown	Ukraine		206638	HOSTFORYUA	true
172.86.188.251	unknown	Canada		32489	AMANAHA-NEWCA	true
50.35.17.13	unknown	United States		27017	ZIPLY-FIBER-LEGACY-ASNUS	true
157.245.99.39	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
75.188.96.231	unknown	United States		10796	TWC-10796-MIDWESTUS	true
167.114.153.111	unknown	Canada		16276	OVHFR	true
37.179.204.33	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
203.153.216.189	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
2.58.16.89	unknown	Latvia		64421	SERTEX-ASLV	true
59.125.219.109	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	true
62.171.142.179	unknown	United Kingdom		51167	CONTABODE	true
123.176.25.234	unknown	Maldives		7642	DHIRAAGU-MV-APDHIVEHIRAAJJEYGEGULHUNPLCMV	true
50.91.114.38	unknown	United States		33363	BHN-33363US	true
61.33.119.226	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
217.123.207.149	unknown	Netherlands		33915	TNF-ASNL	true
78.24.219.147	unknown	Russian Federation		29182	THEFIRST-ASRU	true
173.63.222.65	unknown	United States		701	UUNETUS	true
24.179.13.119	unknown	United States		20115	CHARTER-20115US	true
173.212.214.235	unknown	Germany		51167	CONTABODE	true
47.36.140.164	unknown	United States		20115	CHARTER-20115US	true
110.142.236.207	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
139.99.158.11	unknown	Canada		16276	OVHFR	true
49.50.209.131	unknown	New Zealand		55853	MEGATEL-AS-APMegatelNZ	true
190.108.228.27	unknown	Argentina		27751	NeunetSAAR	true
202.141.243.254	unknown	Pakistan		9260	MULTINET-AS-APMultinetPakistanPvtLtdPK	true
121.124.124.40	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
139.59.60.244	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
61.19.246.238	unknown	Thailand		9335	CAT-CLOUD-APCATTelecomPublicCompanyLimitedTH	true
168.235.67.138	unknown	United States		3842	RAMNODEUS	true
137.59.187.107	unknown	Hong Kong		18106	VIEWQWEST-SG-APViewqwestPteLtdSG	true
78.188.106.53	unknown	Turkey		9121	TTNETTR	true
71.15.245.148	unknown	United States		20115	CHARTER-20115US	true
188.219.31.12	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
217.20.166.178	unknown	Ukraine		1820	WNETUS	true
24.230.141.169	unknown	United States		11232	MIDCO-NETUS	true
74.208.45.104	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
134.209.144.106	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
186.70.56.94	unknown	Ecuador		14522	SatnetEC	true
97.82.79.83	unknown	United States		20115	CHARTER-20115US	true
190.12.119.180	unknown	Argentina		11014	CPSAR	true
139.162.60.124	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	true
172.104.97.173	unknown	United States		63949	LINODE-APLinodeLLCUS	true
184.180.181.202	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
176.113.52.6	unknown	Russian Federation		8712	INTA-ASRU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
201.241.127.190	unknown	Chile		22047	VTRBANDAANCHASACL	true
68.115.186.26	unknown	United States		20115	CHARTER-20115US	true
24.137.76.62	unknown	Canada		11260	EASTLINK-HSICA	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	437123
Start date:	19.06.2021
Start time:	12:34:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bol88C399w.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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
Detection:	MAL
Classification:	mal88.troj.evad.winEXE@9/0@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 46.3% (good quality ratio 40.6%) • Quality average: 61% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 81% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:34:54	API Interceptor	1067x Sleep call for process: splwow64.exe modified
12:35:39	API Interceptor	10x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
216.139.123.119	2ojdmC51As.exe	Get hash	malicious	Browse	
200.116.145.225	2ojdmC51As.exe	Get hash	malicious	Browse	• 200.116.145.225:443/0SatF/P7qctngEpv1Ya3fD3/jr1xjmE/NHdOxCQtbKORku0/xlzXExMFhF/ibPm1TBkGiQpYm/
	GM8716863026AA.doc	Get hash	malicious	Browse	• 200.116.145.225:443/eHRi0AsvmChNb0B/Sq2LBDG3K/dHE8SMLIJOlFGym/g6iocDdP0QPHR/
194.4.58.192	v8iFmF7XPp.dll	Get hash	malicious	Browse	
	2ojdmC51As.exe	Get hash	malicious	Browse	
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	
102.182.93.220	2ojdmC51As.exe	Get hash	malicious	Browse	
95.9.5.93	v8iFmF7XPp.dll	Get hash	malicious	Browse	
	2ojdmC51As.exe	Get hash	malicious	Browse	
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	
94.200.114.161	test-emotet.exe	Get hash	malicious	Browse	• 94.200.114.161/
72.186.136.247	v8iFmF7XPp.dll	Get hash	malicious	Browse	
115.94.207.99	http://https://contentsxx.xsrv.jp/academia/parts_service/7xg/	Get hash	malicious	Browse	• 115.94.207.99:443/OUnj/nu5Sn5pH6W/XCxNN4goRNgqaQshv/BH9p/alZ3dnjhwqocs6Wj/
89.121.205.18	2ojdmC51As.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTER-KZ	jax.k.dll	Get hash	malicious	Browse	• 185.100.65.29
	0519_3361871008218.doc	Get hash	malicious	Browse	• 185.100.65.29
	fax.f.dll	Get hash	malicious	Browse	• 185.100.65.29
	0513_3111026702554.doc	Get hash	malicious	Browse	• 185.100.65.29
	0513_1360918519077.doc	Get hash	malicious	Browse	• 185.100.65.29
	581a98e7_by_Libranalysis.docm	Get hash	malicious	Browse	• 185.100.65.29
	Win32.exe	Get hash	malicious	Browse	• 185.113.134.179
	jers.dll	Get hash	malicious	Browse	• 185.100.65.29
	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 194.4.58.192
	wininit.dll	Get hash	malicious	Browse	• 185.100.65.29
	0408_391585988029.doc	Get hash	malicious	Browse	• 185.100.65.29
	msals.pumpl.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.pumpl.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.dll	Get hash	malicious	Browse	• 185.100.65.29
	NvContainer.exe	Get hash	malicious	Browse	• 185.113.134.179
	0318_45657944978421.doc	Get hash	malicious	Browse	• 185.100.65.29
	2ojdmC51As.exe	Get hash	malicious	Browse	• 194.4.58.192
	FileZilla_3.50.0_win64-setup.exe	Get hash	malicious	Browse	• 185.116.194.200
	0304_87496944093261.doc	Get hash	malicious	Browse	• 185.100.65.29

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0304_56958375050481.doc	Get hash	malicious	Browse	• 185.100.65.29
TTNETTR	invoice-H9247.docx	Get hash	malicious	Browse	• 78.186.110.14
	2dhfmRiWST.exe	Get hash	malicious	Browse	• 85.99.227.85
	aduYorlpGH.exe	Get hash	malicious	Browse	• 85.99.227.85
	sample1.doc	Get hash	malicious	Browse	• 78.186.65.230
	tpdwIENhDh.exe	Get hash	malicious	Browse	• 78.180.177.193
	17D54F646D676B09788537F84FC3BFC8699D78A6B11B9.exe	Get hash	malicious	Browse	• 88.229.252.115
	9cf2c56e_by_Libranalysis.exe	Get hash	malicious	Browse	• 88.249.120.205
	8UsA.sh	Get hash	malicious	Browse	• 78.188.19.132
	nT7K5GG5km	Get hash	malicious	Browse	• 85.110.95.80
	ldr.sh	Get hash	malicious	Browse	• 88.225.138.206
	qJiGYEJs.exe	Get hash	malicious	Browse	• 78.189.219.196
	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 85.105.111.166
	VizZ3QTQMu.exe	Get hash	malicious	Browse	• 195.174.29.189
	g9ldZ16mvPSd1Z1.exe	Get hash	malicious	Browse	• 88.241.166.6
	2ojdmC51As.exe	Get hash	malicious	Browse	• 85.105.111.166
	4xPTS0oLmE.exe	Get hash	malicious	Browse	• 95.14.95.126
	MiAouAtLEk.exe	Get hash	malicious	Browse	• 88.229.0.210
	vB2sN14K0Y.exe	Get hash	malicious	Browse	• 78.189.230.30
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 85.105.111.166
	lo8ic2291n.doc	Get hash	malicious	Browse	• 81.215.230.173
AfrihostZA	BfdkXo6xoH.exe	Get hash	malicious	Browse	• 154.0.171.107
	85cUZZtEFA.xls	Get hash	malicious	Browse	• 154.0.164.210
	85cUZZtEFA.xls	Get hash	malicious	Browse	• 154.0.164.210
	85cUZZtEFA.xls	Get hash	malicious	Browse	• 154.0.164.210
	Document_38047842.xls	Get hash	malicious	Browse	• 154.0.164.210
	Fax_Doc#01_5.html	Get hash	malicious	Browse	• 197.242.146.206
	New Order.exe	Get hash	malicious	Browse	• 154.0.165.45
	sample1.doc	Get hash	malicious	Browse	• 41.76.213.144
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 169.1.24.161
	HU4TEm4Vr7.exe	Get hash	malicious	Browse	• 169.0.142.82
	product specification.xlsx	Get hash	malicious	Browse	• 169.1.24.244
	ppc_unpacked	Get hash	malicious	Browse	• 169.214.149.159
	MGuvcs6Ocz	Get hash	malicious	Browse	• 169.208.248.210
	z3hir.bin	Get hash	malicious	Browse	• 169.128.215.34
	IMG001.exe	Get hash	malicious	Browse	• 169.106.68.226
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 169.1.24.244
	YPJ9DZYIpO	Get hash	malicious	Browse	• 169.107.27.65
	PO#41000055885.exe	Get hash	malicious	Browse	• 154.0.167.80
	2ojdmC51As.exe	Get hash	malicious	Browse	• 102.182.93.220
	Our REVISED Order 1032021.exe	Get hash	malicious	Browse	• 154.0.173.248

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.556948031769578
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	bol88C399w.exe
File size:	581632
MD5:	0a82064af051bad014b77038d60474b6
SHA1:	f7bf190091d5fe307cfaeed630eeb341c935bda0
SHA256:	8f165a26d7e9ad72cb0d51cf01076cc4b0099a244cd4e702645d36dc788dd0cc
SHA512:	8d8c3d9479826597c7cebd1f0c6ff5556af757774af4e606e9958eefd38b93aeacc3142b0eb938430abacdc9c80c84f7fe68bc573cd57faee7612d0b71579302
SSDEEP:	12288:ggyDT8PLvvaKrtURPnMXSVL6ZRwO+4DQDf2TPexaaiWgyDTj1cib:gJDT8PjiKZcPM86rw0WJDTj1cY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.....z.....Rich.....PE..L...B-._..... .....!.....@.....

File Icon

Icon Hash:	60e0e4b4b4cce062

Static PE Info

General

Entrypoint:	0x4021e4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5F992D42 [Wed Oct 28 08:35:14 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ee32a7d07aff9fd88159f3d8028f0500

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6ab00	0x6b000	False	0.600259656104	data	6.95649403306	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x6c000	0x33d0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x20b58	0x21000	False	0.463526870265	data	5.11995480299	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: bol88C399w.exe PID: 7052 Parent PID: 6064

General

Start time:	12:34:53
Start date:	19/06/2021
Path:	C:\Users\user\Desktop\bol88C399w.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\bol88C399w.exe'
Imagebase:	0x400000
File size:	581632 bytes
MD5 hash:	0A82064AF051BAD014B77038D60474B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.663798235.0000000002CC1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000003.658508716.0000000000602000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.661246086.0000000000602000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Deleted

Analysis Process: splwow64.exe PID: 7072 Parent PID: 7052

General

Start time:	12:34:54
Start date:	19/06/2021
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff6fea60000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: KBDHU1.exe PID: 4780 Parent PID: 7052

General

Start time:	12:35:03
Start date:	19/06/2021
Path:	C:\Windows\SysWOW64\mos\KBDHU1.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mos\KBDHU1.exe
Imagebase:	0x400000
File size:	581632 bytes
MD5 hash:	0A82064AF051BAD014B77038D60474B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000003.716674491.00000000032E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.906181296.0000000002341000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.906600906.00000000032D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

Analysis Process: svchost.exe PID: 7108 Parent PID: 568

General

Start time:	12:35:12
Start date:	19/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6812 Parent PID: 568

General

Start time:	12:35:21
Start date:	19/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 7032 Parent PID: 568

General

Start time:	12:35:31
Start date:	19/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5932 Parent PID: 568

General

Start time:	12:35:37
Start date:	19/06/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis