ID: 319735
Sample Name:
2ojdmC51As.exe
Cookbook: default.jbs
Time: 15:59:41
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

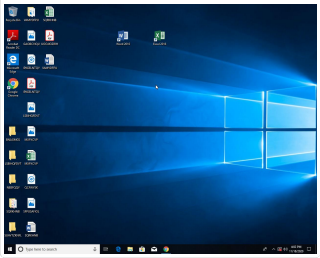
Analysis Report 2ojdmC51As.exe

Overview

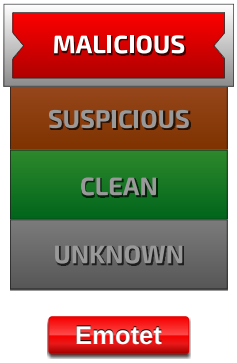
General Information

Sample Name:	2ojdmC51As.exe
Analysis ID:	319735
MD5:	5804d97670dcdfa.
SHA1:	65c817fb511824f..
SHA256:	4e885ada930e28..

Most interesting Screenshot:



Detection

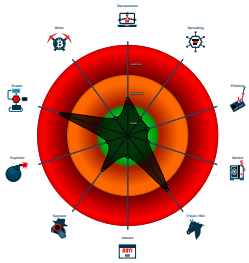


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected Emotet
- Drops executables to the windows d…
- Found evasive API chain (may stop…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Contains capabilities to detect virtua…
- Contains functionality to access load…
- Contains functionality to check if a w…
- Contains functionality to dynamically…
- Contains functionality to enumerate …

Classification



Startup

- **System is w10x64**
- 2ojdmC51As.exe (PID: 6240 cmdline: 'C:\Users\user\Desktop\2ojdmC51As.exe' MD5: 5804D97670DCDFAB88BA830682355DAD)
  - sort.exe (PID: 4564 cmdline: C:\Windows\SysWOW64\setupugc\sort.exe MD5: 5804D97670DCDFAB88BA830682355DAD)
- svchost.exe (PID: 6680 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6748 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7124 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "C2 list": [
    "200.116.145.225:443",
    "96.126.101.6:8080",
    "5.196.108.185:8080",
    "167.114.153.111:8080",
    "194.187.133.160:443",
    "98.174.164.72:80",
    "103.86.49.11:8080",
    "78.24.219.147:8080",
    "50.245.107.73:443",
    "110.145.77.103:80",
    "94.200.114.161:80",
    "61.19.246.238:443",
    "194.4.58.192:7080",
    "209.54.13.14:80",
    "102.182.93.220:80",
    "186.70.56.94:443",
    "203.153.216.189:7080",
    "49.50.209.131:80",
    "176.113.52.6:443",
    "62.30.7.67:443",
    "61.76.222.210:80",
    "113.61.66.94:80",
    "157.245.99.39:8080",
    "216.139.123.119:80",
    "184.180.181.202:80",
    "123.142.37.166:80",
    "124.41.215.226:80",
```

```
"119.59.116.21:8080",
"41.185.28.84:8080",
"5.39.91.110:7080",
"220.245.198.194:80",
"139.162.108.71:8080",
"75.143.247.51:80",
"74.214.230.200:80",
"185.94.252.104:443",
"208.180.207.205:80",
"49.3.224.99:8080",
"93.147.212.206:80",
"182.208.30.18:443",
"95.213.236.64:8080",
"37.187.72.193:8080",
"59.125.219.109:443",
"37.179.204.33:80",
"95.9.5.93:80",
"168.235.67.138:7080",
"118.83.154.64:443",
"121.7.31.214:80",
"74.208.45.104:8080",
"87.106.136.232:8080",
"138.68.87.218:443",
"62.75.141.82:80",
"66.76.12.94:8080",
"202.134.4.216:8080",
"47.36.140.164:80",
"110.142.236.207:80",
"134.209.144.106:443",
"89.216.122.92:80",
"75.188.96.231:80",
"24.179.13.119:80",
"218.147.193.146:80",
"174.106.122.139:80",
"71.15.245.148:8080",
"104.131.11.150:443",
"202.141.243.254:443",
"94.230.70.6:80",
"24.178.90.49:80",
"97.82.79.83:80",
"68.252.26.78:80",
"173.63.222.65:80",
"162.241.242.173:8080",
"79.137.83.50:443",
"80.241.255.202:8080",
"120.150.60.189:80",
"96.245.227.43:80",
"50.91.114.38:80",
"83.110.223.58:443",
"24.230.141.169:80",
"37.139.21.175:8080",
"202.134.4.211:8080",
"190.240.194.77:443",
"176.111.60.55:8080",
"123.176.25.234:80",
"209.141.54.221:7080",
"115.94.207.99:443",
"50.35.17.13:80",
"109.74.5.95:8080",
"120.150.218.241:443",
"121.124.124.40:7080",
"217.20.166.178:7080",
"108.46.29.236:80",
"2.58.16.89:8080",
"85.105.111.166:80",
"137.59.187.107:8080",
"139.162.60.124:8080",
"76.175.162.101:80",
"139.99.158.11:443",
"104.131.123.136:443",
"91.211.88.52:7080",
"91.146.156.228:80",
"172.104.97.173:8080",
"89.121.205.18:80",
"186.74.215.34:80",
"61.33.119.226:443",
"162.241.140.129:8080",
"130.0.132.242:80",
"190.108.228.27:443",
"201.241.127.190:80",
"87.106.139.101:8080",
"78.188.106.53:443",
"188.219.31.12:80",
"76.171.227.238:80",
"72.143.73.234:443",
"62.171.142.179:8080",
"139.59.60.244:8080",
"24.137.76.62:80",
"172.86.188.251:8080",
"172.91.208.86:80",
"94.23.237.171:443",
```

```
"200.116.145.225:443",
"96.126.101.6:8080",
"5.196.108.185:8080",
"167.114.153.111:8080",
"194.187.133.160:443",
"98.174.164.72:80",
"103.86.49.11:8080",
"78.24.219.147:8080",
"50.245.107.73:443",
"110.145.77.103:80",
"94.200.114.161:80",
"61.19.246.238:443",
"194.4.58.192:7080",
"209.54.13.14:80",
"102.182.93.220:80",
"186.70.56.94:443",
"203.153.216.189:7080",
"49.50.209.131:80",
"176.113.52.6:443",
"62.30.7.67:443",
"61.76.222.210:80",
"113.61.66.94:80",
"157.245.99.39:8080",
"216.139.123.119:80",
"184.180.181.202:80",
"123.142.37.166:80",
"124.41.215.226:80",
"119.59.116.21:8080",
"41.185.28.84:8080",
"5.39.91.110:7080",
"220.245.198.194:80",
"139.162.108.71:8080",
"75.143.247.51:80",
"74.214.230.200:80",
"185.94.252.104:443",
"208.180.207.205:80",
"49.3.224.99:8080",
"93.147.212.206:80",
"182.208.30.18:443",
"95.213.236.64:8080",
"37.187.72.193:8080",
"59.125.219.109:443",
"37.179.204.33:80",
"95.9.5.93:80",
"168.235.67.138:7080",
"118.83.154.64:443",
"121.7.31.214:80",
"74.208.45.104:8080",
"87.106.136.232:8080",
"138.68.87.218:443",
"62.75.141.82:80",
"66.76.12.94:8080",
"202.134.4.216:8080",
"47.36.140.164:80",
"110.142.236.207:80",
"134.209.144.106:443",
"89.216.122.92:80",
"75.188.96.231:80",
"24.179.13.119:80",
"218.147.193.146:80",
"174.106.122.139:80",
"71.15.245.148:8080",
"104.131.11.150:443",
"202.141.243.254:443",
"94.230.70.6:80",
"24.178.90.49:80",
"97.82.79.83:80",
"68.252.26.78:80",
"173.63.222.65:80",
"162.241.242.173:8080",
"79.137.83.50:443",
"80.241.255.202:8080",
"120.150.60.189:80",
"96.245.227.43:80",
"50.91.114.38:80",
"83.110.223.58:443",
"24.230.141.169:80",
"37.139.21.175:8080",
"202.134.4.211:8080",
"190.240.194.77:443",
"176.111.60.55:8080",
"123.176.25.234:80",
"209.141.54.221:7080",
"115.94.207.99:443",
"50.35.17.13:80",
"109.74.5.95:8080",
"120.150.218.241:443",
"121.124.124.40:7080",
"217.20.166.178:7080",
"108.46.29.236:80",
"2.58.16.89:8080",
```

```
    "85.105.111.166:80",
    "137.59.187.107:8080",
    "139.162.60.124:8080",
    "76.175.162.101:80",
    "139.99.158.11:443",
    "104.131.123.136:443",
    "91.211.88.52:7080",
    "91.146.156.228:80",
    "172.104.97.173:8080",
    "89.121.205.18:80",
    "186.74.215.34:80",
    "61.33.119.226:443",
    "162.241.140.129:8080",
    "130.0.132.242:80",
    "190.108.228.27:443",
    "201.241.127.190:80",
    "87.106.139.101:8080",
    "78.188.106.53:443",
    "188.219.31.12:80",
    "76.171.227.238:80",
    "72.143.73.234:443",
    "62.171.142.179:8080",
    "139.59.60.244:8080",
    "24.137.76.62:80",
    "172.86.188.251:8080",
    "172.91.208.86:80",
    "94.23.237.171:443"
  ],
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhANQOcBKvh5xEW7VcJ9totsjdBwuAclxS\nQ0e09fk8V053lktpW3TRrzAW63yt6j1KWnyxMrU3igFXypBoI4lVNmkje4UPtIIS\nfkzjEIvG1v/ZNn1k0J0PfFTxbFFeUEs3AwIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.931629655.0000000002220000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.667768852.0000000000664000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.931663752.0000000002244000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.667968476.0000000002231000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.931690638.0000000002271000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Unpacked PEs

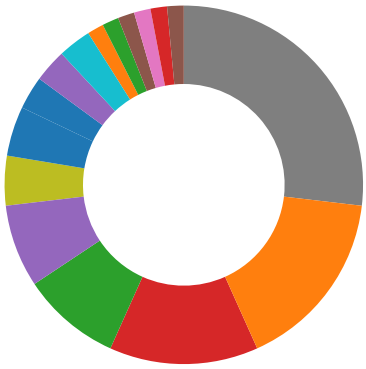
Source	Rule	Description	Author	Strings
0.2.2ojdmC51As.exe.2230000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.sort.exe.2270000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Spreading
- Networking



- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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)

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Stealing of Sensitive Information:

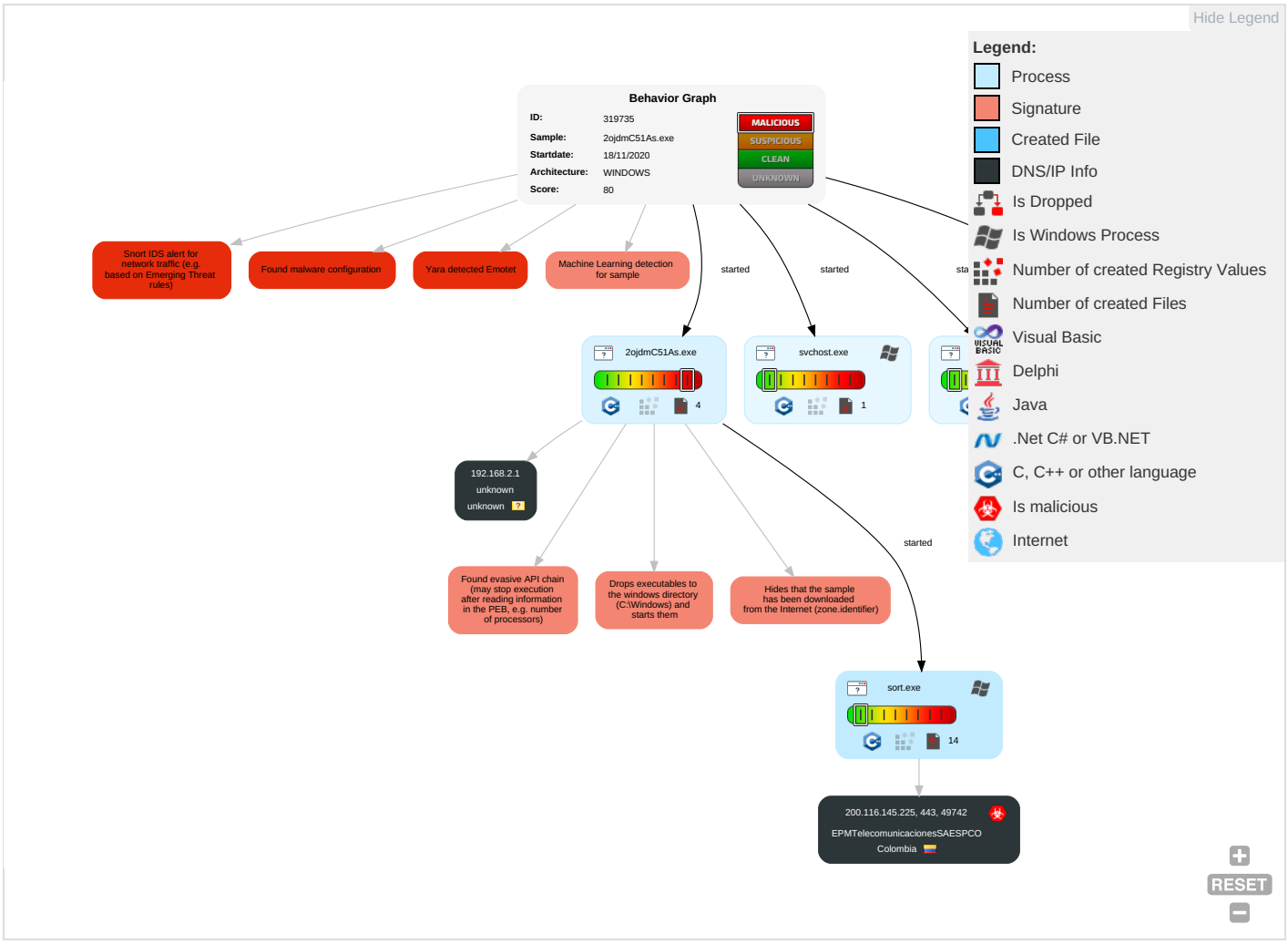
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Service Execution 1	Windows Service 2	Windows Service 2	Masquerading 1 2	Input Capture 2	System Time Discovery 2	Remote Services	Input Capture 2	Exfiltration Over Other Network Medium	Encrypted Channel 2 2	Eavesdrop on Insecure Network Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 2	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Service Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 6	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station

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
2ojdmC51As.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.2ojdmC51As.exe.2230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.sort.exe.2270000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://200.116.145.225:443/0SatF/P7qctngEpv1Ya3fD3/jr1xjmE/NHdOxCQtbKORku0/xlzXExMFhF/ibPm1TBkGiQpYm	0%	Avira URL Cloud	safe	
http://https://200.116.145.225:443/0SatF/P7qctngEpv1Ya3fD3/jr1xjmE/NHdOxCQtbKORku0/xlzXExMFhF/ibPm1TBkGiQpYm/	0%	Avira URL Cloud	safe	
http://https://watson.telemet:443/0SatF/P7qctngEpv1Ya3fD3/jr1xjmE/NHdOxCQtbKORku0/xlzXExMFhF/ibPm1TBkGiQpYm	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://200.116.145.225:443/0SatF/P7qctngEpv1Ya3fD3/jr1xjmE/NHdOxCQtbKORku0/xlzXExMFhF/ibPm1TBkGiQpYm/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hulu.com/privacy	svchost.exe, 00000006.00000003.752710199.0000027873F8F000.00000004.00000001.sdmp	false		high
http://200.116.145.225:443/0SatF/P7qctngEpv1Ya3fD3/jr1xjmE/NHdOxCQtbKORku0/xlzXExMFhF/ibPm1TBkGiQpYm	sort.exe, 00000001.00000002.932263156.0000000002AA3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 00000006.00000003.753653199.0000027873F79000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.753689942.0000027873F58000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/do-not-sell-my-info	svchost.exe, 00000006.00000003.752710199.0000027873F8F000.00000004.00000001.sdmp	false		high
http://www.hulu.com/terms	svchost.exe, 00000006.00000003.752710199.0000027873F8F000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 00000006.00000003.758203492.0000027873F2A000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.758104226.0000027873F6B000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/develop	svchost.exe, 00000006.00000003.758203492.0000027873F2A000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.758104226.0000027873F6B000.00000004.00000001.sdmp	false		high
http://universalstore.streaming.mediaservices.windows.net/411ee20d-d1b8-4d57-ae3f-af22235d79d9/1f8e1	svchost.exe, 00000006.00000003.758203492.0000027873F2A000.00000004.00000001.sdmp	false		high
http://https://instagram.com/hiddencity_	svchost.exe, 00000006.00000003.753653199.0000027873F79000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.753689942.0000027873F58000.00000004.00000001.sdmp	false		high
http://https://watson.telemet:443/0SatF/P7qctngEpv1Ya3fD3/jr1xjmE/NHdOxCQtbKORku0/xlzXExMFhF/ibPm1TBkGiQpYm	sort.exe, 00000001.00000002.932252355.0000000002A7F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.roblox.com/info/privacy	svchost.exe, 00000006.00000003.758203492.0000027873F2A000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.758104226.0000027873F6B000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.g5e.com/termsofservice	svchost.exe, 00000006.00000003.753653199.0000027873F79000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.753689942.0000027873F58000.00000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 00000006.00000003.758203492.0000027873F2A000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.758104226.0000027873F6B000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/parents/	svchost.exe, 00000006.00000003.758203492.0000027873F2A000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.758104226.0000027873F6B000.00000004.00000001.sdmp, svchost.exe, 00000006.00000003.758139074.0000027873F62000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/ca-privacy-rights	svchost.exe, 00000006.00000003.752710199.0000027873F8F000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
200.116.145.225	unknown	Colombia		13489	EPMTelecomunicacionesSA ESPCO	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319735
Start date:	18.11.2020
Start time:	15:59:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2ojdmC51As.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:	14
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:	mal80.troj.evad.winEXE@6/0@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 65.4% (good quality ratio 64.7%) • Quality average: 85% • Quality standard deviation: 22.1%
HCA Information:	• Successful, ratio: 86% • 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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 51.104.139.180, 52.155.217.156, 20.54.26.129, 67.26.137.254, 8.241.11.126, 8.248.133.254, 8.253.204.249, 8.253.204.121, 92.122.213.247, 92.122.213.194, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/319735/sample/2ojdmC51As.exe

Simulations

Behavior and APIs

Time	Type	Description
16:01:17	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
200.116.145.225	GM8716863026AA.doc	Get hash	malicious	Browse	• 200.116.145.225:443/eHRi0AsvmChNb0B/Sq2LBDG3K/dHE8SMLlJOlFGym/g6iocDdP0QPHR/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EPMTelecomunicacionesSAESPCO	A8732vSTKW.exe	Get hash	malicious	Browse	• 181.129.134.18
	pIxnU8KH8P.exe	Get hash	malicious	Browse	• 181.129.134.18
	4UwAHMfQ1s.exe	Get hash	malicious	Browse	• 181.129.104.139
	8vjs9LBNaU.exe	Get hash	malicious	Browse	• 181.129.134.18
	zL474n0Mst.exe	Get hash	malicious	Browse	• 200.116.145.225
	z9dSgDlbe1.exe	Get hash	malicious	Browse	• 200.116.145.225
	0FzZuRH6Gy.exe	Get hash	malicious	Browse	• 200.116.145.225
	JdjCbjCf.exe	Get hash	malicious	Browse	• 201.232.179.81
	qwhWqUYlnN.exe	Get hash	malicious	Browse	• 181.143.194.138
	7U0Y1bRt9b.exe	Get hash	malicious	Browse	• 200.116.232.186
	zLjBdL6Lbk.exe	Get hash	malicious	Browse	• 181.129.93.226
	GM8716863026AA.doc	Get hash	malicious	Browse	• 200.116.145.225
	a.exe	Get hash	malicious	Browse	• 200.122.209.78
	SecuriteInfo.com.Trojan.GenericKDZ.69690.30809.exe	Get hash	malicious	Browse	• 181.129.104.139
	SecuriteInfo.com.Trojan.GenericKDZ.69690.25514.exe	Get hash	malicious	Browse	• 181.129.134.18
	Archivo Pdf.exe	Get hash	malicious	Browse	• 181.140.213.213
	14082020 PDF.exe	Get hash	malicious	Browse	• 181.140.213.213
	Solicitud.exe	Get hash	malicious	Browse	• 181.140.213.213
	CITA FISCAL N#U00ba 00964673335 15 ABRIL DE 2020.exe	Get hash	malicious	Browse	• 181.141.10.15
	9459cddst.exe	Get hash	malicious	Browse	• 200.116.232.186

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):	7.0032331918802715
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	2ojdmC51As.exe
File size:	376832
MD5:	5804d97670dcdfab88ba830682355dad
SHA1:	65c817fb511824fa185f34ecd744b836ed7a19eb
SHA256:	4e885ada930e285a005c5211b8a652dc0eb11a06ccf530561afa88aefe99c9fc
SHA512:	befd479d37ff5bef768d61aeec101b4f584e8519f4b3d60f6f0692614ce8925a8303ae478b4d21652b64bc36bc38e9d2eb44d874c2f973f310f2e8ff2a0c7a4
SSDEEP:	6144:HzoTjUrx4KVHa9eUfTLHy2VrH0D+wieIMl7lT2IcO/wksAPJLzx:ToCHVcjZwie57l6i/wi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!..`r..`r..`r..`r..`r..sr..`r..as..`r..arC.`rp.nr..`r..jr..`r..kr..`rK.fr..`rRich..`r.....PE..L....._.....

File Icon

	
Icon Hash:	71b018ccc6577131

Static PE Info

General

Entrypoint:	0x406388
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:	0x5F920784 [Thu Oct 22 22:28:20 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:	875a1634331d344707689db6d9489063

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 0042F100h
push 00409800h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 58h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
call dword ptr [0042B2CCh]
xor edx, edx
mov dl, ah
mov dword ptr [00439D04h], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [00439D00h], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [00439CFCh], ecx
shr eax, 10h
mov dword ptr [00439CF8h], eax
push 00000001h
call 00007F25005A0C0Eh
pop ecx
test eax, eax
jne 00007F250059F68Ah
push 0000001Ch
call 00007F250059F748h
pop ecx
call 00007F25005A2079h
test eax, eax
jne 00007F250059F68Ah
push 00000010h
call 00007F250059F737h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007F25005A28B2h
call dword ptr [0042B1D0h]
mov dword ptr [0043B87Ch], eax
call 00007F25005A2770h
mov dword ptr [00439CE8h], eax
call 00007F25005A2519h
call 00007F25005A245Bh
call 00007F250059F86Ch
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [0042B1D4h]
call 00007F25005A23ECh
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007F250059F688h
movzx eax, word ptr [ebp+00h]

Rich Headers

Programming Language:	• [C] VS98 (6.0) build 8168 • [RES] VS98 (6.0) cvtres build 1720 • [C++] VS98 (6.0) build 8168

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x33a68	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c000	0x23812	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2b000	0x5c8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x29ef1	0x2a000	False	0.574718656994	data	6.56296579611	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2b000	0xa8be	0xb000	False	0.309792258523	data	4.42786700159	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x36000	0x5890	0x2000	False	0.253784179688	data	3.64382398996	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x3c000	0x23812	0x24000	False	0.909579806858	data	7.73501222548	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x3c8e0	0x134	data	English	United States
RT_CURSOR	0x3ca14	0xb4	data	English	United States
RT_CURSOR	0x3cac8	0x134	data	English	United States
RT_CURSOR	0x3cbfc	0xb4	data	English	United States
RT_ICON	0x3ccb0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	English	United States
RT_ICON	0x3cf98	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x3d0c0	0x2e8	data	English	United States
RT_ICON	0x3d3a8	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_MENU	0x3d4d0	0x23e	data	English	United States
RT_STRING	0x3d710	0x90	data	English	United States
RT_STRING	0x3d7a0	0x3e	data	English	United States
RT_STRING	0x3d7e0	0x296	data	English	United States
RT_STRING	0x3da78	0x260	data	English	United States
RT_STRING	0x3dcd8	0x328	data	English	United States
RT_STRING	0x3e000	0x70	data	English	United States
RT_STRING	0x3e070	0x106	data	English	United States
RT_STRING	0x3e178	0xda	data	English	United States
RT_STRING	0x3e254	0x46	data	English	United States
RT_STRING	0x3e29c	0xc6	data	English	United States
RT_STRING	0x3e364	0x1f8	data	English	United States
RT_STRING	0x3e55c	0x86	data	English	United States
RT_STRING	0x3e5e4	0xd0	data	English	United States
RT_STRING	0x3e6b4	0x2a	data	English	United States
RT_STRING	0x3e6e0	0x14a	data	English	United States
RT_STRING	0x3e82c	0x124	data	English	United States
RT_STRING	0x3e950	0x4e2	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x3ee34	0x2a2	data	English	United States
RT_STRING	0x3f0d8	0x2dc	data	English	United States
RT_STRING	0x3f3b4	0xac	data	English	United States
RT_STRING	0x3f460	0xde	data	English	United States
RT_STRING	0x3f540	0x4c4	data	English	United States
RT_STRING	0x3fa04	0x264	data	English	United States
RT_STRING	0x3fc68	0x2c	data	English	United States
RT_ACCELERATOR	0x3fc94	0x70	data	English	United States
RT_ACCELERATOR	0x3fd04	0x18	data	English	United States
RT_RCDATA	0x3fd1c	0x1f733	data	English	United States
RT_GROUP_CURSOR	0x5f450	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x5f474	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_ICON	0x5f498	0x22	data	English	United States
RT_GROUP_ICON	0x5f4bc	0x22	data	English	United States
RT_VERSION	0x5f4e0	0x314	data	English	United States
None	0x5f7f4	0x1e	data	English	United States

Imports

DLL	Import
KERNEL32.dll	VirtualFree, IsBadWritePtr, UnhandledExceptionFilter, FreeEnvironmentStringsA, FreeEnvironmentStringsW, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetStdHandle, GetFileType, SetUnhandledExceptionFilter, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, HeapCreate, IsBadCodePtr, SetStdHandle, CompareStringA, CompareStringW, SetEnvironmentVariableA, HeapDestroy, GetACP, HeapSize, HeapReAlloc, RaiseException, TerminateProcess, ExitProcess, GetCommandLineA, GetStartupInfoA, HeapFree, InterlockedExchange, GetLocalTime, GetSystemTime, GetTimeZoneInformation, RtlUnwind, HeapAlloc, FileTimeToLocalFileTime, FileTimeToSystemTime, SetErrorMode, SystemTimeToFileTime, LocalFileTimeToFileTime, GetFileSize, GetVolumeInformationA, FindFirstFileA, FindClose, DeleteFileA, MoveFileA, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, CreateFileA, DuplicateHandle, GetOEMCP, GetCPInfo, GetProcessVersion, WritePrivateProfileStringA, TlsGetValue, LocalReAlloc, TlsSetValue, EnterCriticalSection, GlobalReAlloc, LeaveCriticalSection, TlsFree, GlobalHandle, DeleteCriticalSection, TlsAlloc, InitializeCriticalSection, LocalFree, LocalAlloc, WideCharToMultiByte, InterlockedIncrement, GlobalFlags, InterlockedDecrement, GetLastError, SetLastError, MulDiv, lstrlenA, MultiByteToWideChar, GetDiskFreeSpaceA, GetFileTime, SetFileTime, GetFullPathNameA, GetTempFileNameA, lstrcpynA, GetFileAttributesA, FreeLibrary, GetVersion, lstrcatA, GlobalGetAtomNameA, GlobalAddAtomA, GlobalFindAtomA, lstrcpyA, GetModuleHandleA, CloseHandle, GetModuleFileNameA, GlobalAlloc, GlobalDeleteAtom, lstrcmpiA, GetCurrentThread, GetCurrentThreadId, lstrcmpA, GlobalLock, GlobalUnlock, GlobalFree, LockResource, FindResourceA, LoadResource, GetTickCount, Sleep, LoadLibraryA, VirtualAlloc, GetModuleHandleExA, GetProcAddress, GetCurrentProcess, IsBadReadPtr
USER32.dll	TranslateAcceleratorA, ReleaseCapture, GetDesktopWindow, DestroyMenu, LoadMenuA, SetMenu, ReuseDDElParam, UnpackDDElParam, BringWindowToTop, ClientToScreen, GetWindowDC, BeginPaint, EndPaint, TabbedTextOutA, DrawTextA, GrayStringA, IsZoomed, SetParent, IsRectEmpty, AppendMenuA, DeleteMenu, GetSystemMenu, GetClassNameA, GetSysColorBrush, LoadStringA, CharUpperA, FindWindowA, GetTabbedTextExtentA, KillTimer, WindowFromPoint, InflateRect, SetCapture, InvertRect, GetDCEx, LockWindowUpdate, GetDC, ReleaseDC, LoadCursorA, DestroyCursor, ShowWindow, SetWindowTextA, IsDialogMessageA, SetDlgItemTextA, LoadIconA, UpdateWindow, SendDlgItemMessageA, MapWindowPoints, GetSysColor, SetFocus, AdjustWindowRectEx, ScreenToClient, EqualRect, DeferWindowPos, BeginDeferWindowPos, CopyRect, EndDeferWindowPos, ScrollWindow, GetScrollInfo, LoadAcceleratorsA, ShowScrollBar, GetScrollRange, SetScrollRange, GetScrollPos, SetScrollPos, GetTopWindow, IsChild, GetCapture, WinHelpA, wsprintfA, GetClassInfoA, RegisterClassA, GetMenu, GetMenuItemCount, GetSubMenu, GetWindowTextLengthA, GetWindowTextA, GetDlgCtrlID, DefWindowProcA, CreateWindowExA, GetClassLongA, SetPropA, UnhookWindowsHookEx, GetPropA, CallWindowProcA, RemovePropA, GetMessageTime, GetMessagePos, GetForegroundWindow, SetForegroundWindow, GetWindow, SetWindowLongA, SetWindowPos, RegisterWindowMessageA, OffsetRect, IntersectRect, SystemParametersInfoA, IsIconic, GetWindowPlacement, GetWindowRect, GetMenuCheckMarkDimensions, GetMenuState, ModifyMenuA, SetMenuItemBitmaps, CheckMenuItem, EnableMenuItem, GetFocus, GetKeyState, CallNextHookEx, ValidateRect, IsWindowVisible, GetCursorPos, SetWindowsHookExA, GetLastActivePopup, MessageBoxA, SetCursor, ShowOwnedPopups, PostMessageA, PostQuitMessage, GetNextDlgTabItem, EndDialog, GetActiveWindow, SetActiveWindow, IsWindow, GetSystemMetrics, CreateDialogIndirectParamA, DestroyWindow, GetParent, GetWindowLongA, GetDlgItem, IsWindowEnabled, SetRectEmpty, PtInRect, FillRect, SetScrollInfo, SetRect, SendMessageA, PeekMessageA, GetMessageA, TranslateMessage, DispatchMessageA, SetTimer, InvalidateRect, GetClientRect, LoadBitmapA, EnableWindow, GetMenuItemID, UnregisterClassA
GDI32.dll	GetDeviceCaps, PatBlt, GetStockObject, Rectangle, DPtoLP, CreatePen, GetViewportOrgEx, AbortDoc, EndDoc, EndPage, StartPage, StartDocA, SetAbortProc, CreateDCA, SaveDC, RestoreDC, SetBkMode, SetPolyFillMode, SetROP2, SetStretchBltMode, SetMapMode, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowOrgEx, SetWindowExtEx, ScaleWindowExtEx, SelectClipRgn, ExcludeClipRect, IntersectClipRect, MoveToEx, LineTo, SetTextAlign, GetCurrentPositionEx, GetObjectA, CreateRectRgn, GetViewportExtEx, GetWindowExtEx, CreateSolidBrush, CreatePatternBrush, PtVisible, RectVisible, TextOutA, ExtTextOutA, Escape, GetTextExtentPoint32A, GetTextMetricsA, StretchDIBits, GetCharWidthA, CreateFontA, CreateFontIndirectA, LPtoDP, GetBkColor, GetNearestColor, GetTextColor, GetStretchBltMode, GetPolyFillMode, GetTextAlign, GetBkMode, GetROP2, GetTextFaceA, GetWindowOrgEx, SetRectRgn, CombineRgn, CreateRectRgnIndirect, SetTextColor, SetBkColor, GetClipBox, CreateBitmap, CreateCompatibleBitmap, SelectObject, StretchBlt, DeleteObject, DeleteDC, BitBlt, CreateCompatibleDC
comdlg32.dll	GetFileTitleA, PrintDlgA, CommDlgExtendedError, GetSaveFileNameA, GetOpenFileNameA
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter

DLL	Import
ADVAPI32.dll	RegQueryValueExA, RegOpenKeyExA, RegCreateKeyExA, RegCloseKey, GetFileSecurityA, SetFileSecurityA, RegSetValueExA
SHELL32.dll	DragQueryFileA, DragFinish
COMCTL32.dll	

Version Infos

Description	Data
LegalCopyright	Copyright (C) 2003
InternalName	EffectDemo
FileVersion	1, 0, 0, 1
CompanyName	
LegalTrademarks	
ProductName	EffectDemo Application
ProductVersion	1, 0, 0, 1
FileDescription	EffectDemo MFC Application
OriginalFilename	EffectDemo.EXE
Translation	0x0409 0x04b0

Possible Origin

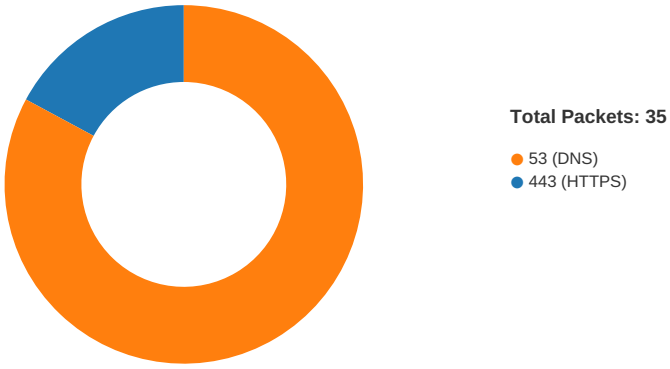
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/18/20-16:00:56.201479	TCP	2404324	ET CNC Feodo Tracker Reported CnC Server TCP group 13	49742	443	192.168.2.4	200.116.145.225

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:00:56.201478958 CET	49742	443	192.168.2.4	200.116.145.225
Nov 18, 2020 16:00:56.396552086 CET	443	49742	200.116.145.225	192.168.2.4
Nov 18, 2020 16:00:56.396764040 CET	49742	443	192.168.2.4	200.116.145.225
Nov 18, 2020 16:00:56.398037910 CET	49742	443	192.168.2.4	200.116.145.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:00:56.398277044 CET	49742	443	192.168.2.4	200.116.145.225
Nov 18, 2020 16:00:56.595930099 CET	443	49742	200.116.145.225	192.168.2.4
Nov 18, 2020 16:00:56.595947981 CET	443	49742	200.116.145.225	192.168.2.4
Nov 18, 2020 16:00:56.783943892 CET	443	49742	200.116.145.225	192.168.2.4
Nov 18, 2020 16:00:57.383925915 CET	443	49742	200.116.145.225	192.168.2.4
Nov 18, 2020 16:00:57.384022951 CET	49742	443	192.168.2.4	200.116.145.225
Nov 18, 2020 16:02:02.399162054 CET	443	49742	200.116.145.225	192.168.2.4
Nov 18, 2020 16:02:02.399306059 CET	49742	443	192.168.2.4	200.116.145.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:00:33.099268913 CET	52991	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:33.134911060 CET	53	52991	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:33.932281017 CET	53700	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:33.959232092 CET	53	53700	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:35.197410107 CET	51726	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:35.224631071 CET	53	51726	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:35.978636026 CET	56794	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:36.005954027 CET	53	56794	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:37.021862030 CET	56534	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:37.048950911 CET	53	56534	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:38.367702007 CET	56627	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:38.394817114 CET	53	56627	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:39.535403967 CET	56621	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:39.562432051 CET	53	56621	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:40.350146055 CET	63116	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:40.377121925 CET	53	63116	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:41.208791018 CET	64078	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:41.237062931 CET	53	64078	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:42.726011038 CET	64801	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:42.753050089 CET	53	64801	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:43.777288914 CET	61721	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:43.804213047 CET	53	61721	8.8.8.8	192.168.2.4
Nov 18, 2020 16:00:59.555849075 CET	51255	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:00:59.583035946 CET	53	51255	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:16.963365078 CET	61522	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:16.990312099 CET	53	61522	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:17.522742987 CET	52337	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:17.558396101 CET	53	52337	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:17.987303019 CET	55046	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:18.022695065 CET	53	55046	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:18.325546026 CET	49612	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:18.360960007 CET	53	49612	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:18.643338919 CET	49285	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:18.670428991 CET	53	49285	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:18.853090048 CET	50601	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:18.888967037 CET	53	50601	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:19.287672997 CET	60875	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:19.314896107 CET	53	60875	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:19.729796886 CET	56448	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:19.765239000 CET	53	56448	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:20.354146004 CET	59172	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:20.381256104 CET	53	59172	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:21.001224041 CET	62420	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:21.036653996 CET	53	62420	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:21.382581949 CET	60579	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:21.409843922 CET	53	60579	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:21.519098043 CET	50183	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:21.546266079 CET	53	50183	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:33.886970043 CET	61531	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:33.914041042 CET	53	61531	8.8.8.8	192.168.2.4
Nov 18, 2020 16:01:34.217612028 CET	49228	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:34.244699955 CET	53	49228	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:01:38.323909044 CET	59794	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:01:38.360553026 CET	53	59794	8.8.8.8	192.168.2.4
Nov 18, 2020 16:02:10.261842012 CET	55916	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:02:10.289072037 CET	53	55916	8.8.8.8	192.168.2.4
Nov 18, 2020 16:02:12.596378088 CET	52752	53	192.168.2.4	8.8.8.8
Nov 18, 2020 16:02:12.623620033 CET	53	52752	8.8.8.8	192.168.2.4

HTTP Request Dependency Graph

- 200.116.145.225
  - 200.116.145.225:443

HTTP Packets

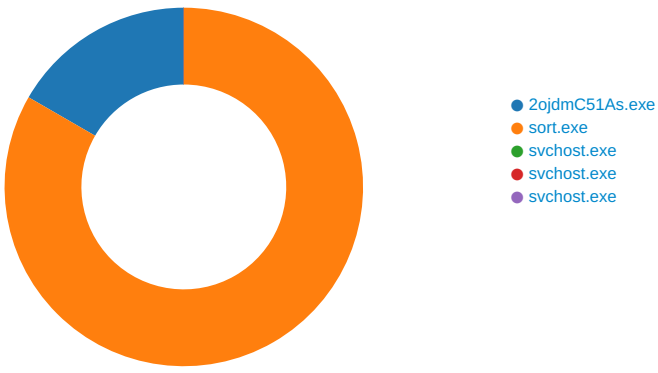
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49742	200.116.145.225	443	C:\Windows\SysWOW64\setupugc\sort.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2020 16:00:56.398037910 CET	157	OUT	POST /0SatF/P7qctngEpv1Ya3fD3/jr1xjmE/NHdOxCQtbKORku0/xlzXExMFhF/ibPm1TBkGiQpYm/ HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Encoding: gzip, deflate DNT: 1 Connection: keep-alive Referer: 200.116.145.225/ Upgrade-Insecure-Requests: 1 Content-Type: multipart/form-data; boundary=---------hcIbcONok User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 200.116.145.225:443 Content-Length: 4628 Cache-Control: no-cache
Nov 18, 2020 16:00:57.383925915 CET	162	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 18 Nov 2020 15:00:57 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 132 Connection: keep-alive Data Raw: 86 2d 97 64 dc 2f f8 df 14 38 07 51 47 c3 82 1e 9f a3 ba c8 d0 2b 43 69 bb 3b 52 61 27 3f 2a 29 23 ca ab b4 0c 87 79 27 e5 f8 12 aa 34 a6 67 1b cb d6 18 b7 d9 cd 1f 7e a9 3e d8 f6 74 85 25 34 ef 26 d3 d4 a7 7d dd 72 9d 53 6e ab e6 41 e3 1b 5d 14 0c 65 04 51 c3 9d 16 cd 48 17 e8 f2 17 79 96 33 16 89 ac 54 9d a3 23 36 b4 bc b1 be 1e e3 7b 1d ff ee 1e 79 1a 06 83 d0 8d 69 25 22 4a 20 90 a6 98 c3 Data Ascii: -d/8QG+Ci;Ra'?*)#y'4g~>t%4&}rSnA]eQHy3T#6{yi%"J

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 2ojdmC51As.exe PID: 6240 Parent PID: 5864

General

Start time:	16:00:37
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\2ojdmC51As.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\2ojdmC51As.exe'
Imagebase:	0x400000
File size:	376832 bytes
MD5 hash:	5804D97670DCDFAB88BA830682355DAD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.667768852.0000000000664000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.667968476.0000000002231000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.667721626.0000000000620000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4013FC	CreateDirectoryA
C:\ProgramData\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40175C	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\setupugc\sort.exe:Zone.Identifier	success or wait	1	2233779	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: sort.exe PID: 4564 Parent PID: 6240

General

Start time:	16:00:38
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\setupugc\sort.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\setupugc\sort.exe
Imagebase:	0x400000
File size:	376832 bytes
MD5 hash:	5804D97670DCDFAB88BA830682355DAD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.931629655.0000000002220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.931663752.0000000002244000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.931690638.0000000002271000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4013FC	CreateDirectoryA
C:\ProgramData\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40175C	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2272CD7	HttpSendRequestW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\setupugc\sort.exe	cannot delete	1	2277EA8	DeleteFileW

Analysis Process: svchost.exe PID: 6680 Parent PID: 568

General

Start time:	16:00:59
Start date:	18/11/2020
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6748 Parent PID: 568

General

Start time:	16:01:07
Start date:	18/11/2020
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 7124 Parent PID: 568

General

Start time:	16:01:15
Start date:	18/11/2020
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis