ID: 679121
Sample Name:
#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe
Cookbook: default.jbs
Time: 09:51:09
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

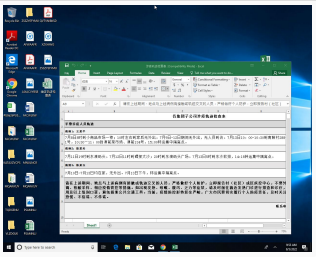
Windows Analysis Report

#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe

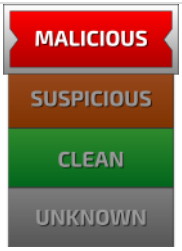
Overview

General Information

Sample Name:	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe
Analysis ID:	679121
MD5:	2d2e2831ae6351.
SHA1:	52a95894b85517.
SHA256:	ffeb7d694c82c2d..
Tags:	exe
Infos:	



Detection



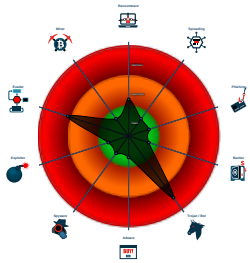
CobaltStrike

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected CobaltStrike
- C2 URLs / IPs found in malware con…
- Uses an obfuscated file name to hid…
- Yara signature match
- PE file contains strange resources
- Tries to load missing DLLs
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Sample execution stops while proce…
- Tries to resolve domain names, but

Classification



Process Tree

- **System is w10x64**
- #U8d26#U53f7#U5bc6#U7801#U8868.xls.exe (PID: 5940 cmdline: "C:\Users\user\Desktop\#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe" MD5: 2D2E2831AE6351FBEE7810BFC0D10955)
  - cmd.exe (PID: 5828 cmdline: c:\windows\system32\cmd.exe /C start ???????.xls MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 4540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - EXCEL.EXE (PID: 5232 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /dde MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

Threatname: CobaltStrike

```
{
  "C2Server": "http://jquery-min.us:8443/jquery-3.3.2.slim.min.js",
  "User Agent": "User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko\r\n"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp	Cobaltbaltstrike_RAW_Payload_https_stager_x64	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x4000:$h01: FC 48 83 E4 F0 E8 C8 00 00 00 41 51 41 50 52 51 56 48 31 D2 65 48 8B 52

Source	Rule	Description	Author	Strings
00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp	Cobaltbaltstrike_Payload_Encoded	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x3400:$s10: /EiD5PDoyAAAAEFRQVBSUVZIMdJlSItSYEiLUhhli1IgSItyUEgPt0pKTTHJSDHA • 0x3900:$s10: /EiD5PDoyAAAAEFRQVBSUVZIMdJlSItSYEiLUhhli1IgSItyUEgPt0pKTTHJSDHA
00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_CobaltStrike_3	Yara detected CobaltStrike	Joe Security	
00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_CobaltStrike	Yara detected CobaltStrike	Joe Security	
00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp	Windows_Trojan_Metasploit_7bc0f998	Identifies the API address lookup function leverage by metasploit shellcode	unknown	• 0x4011:$a1: 48 31 D2 65 48 8B 52 60 48 8B 52 18 48 8B 52 20 48 8B 72 50 48 0F B7 4A 4A 4D 31 C9 48 31 C0 AC 3C 61
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

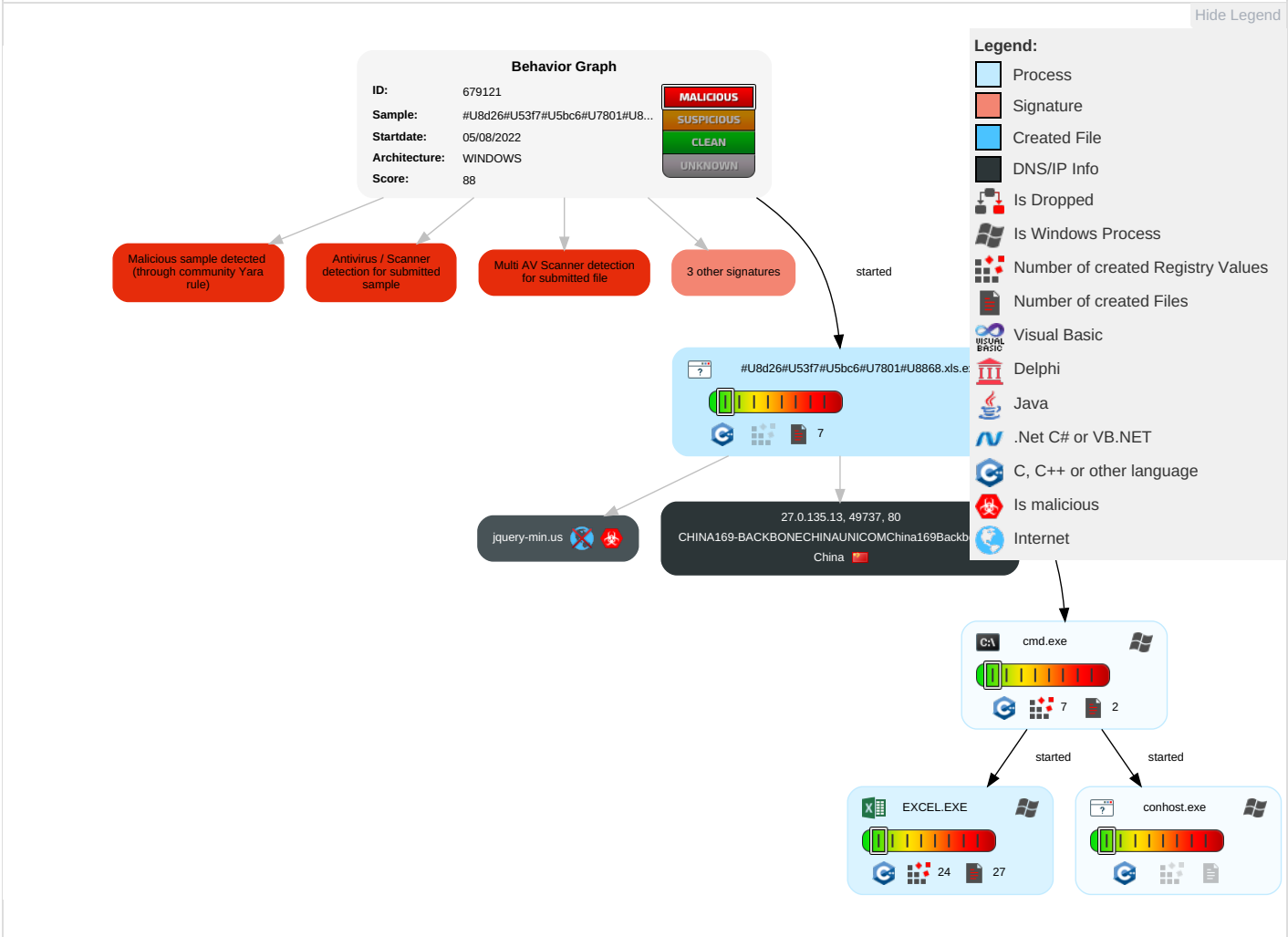
Remote Access Functionality

Yara detected CobaltStrike

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 DLL Side-Loading	1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Process Injection	LSASS Memory	1 Remote System Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	NTDS	2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

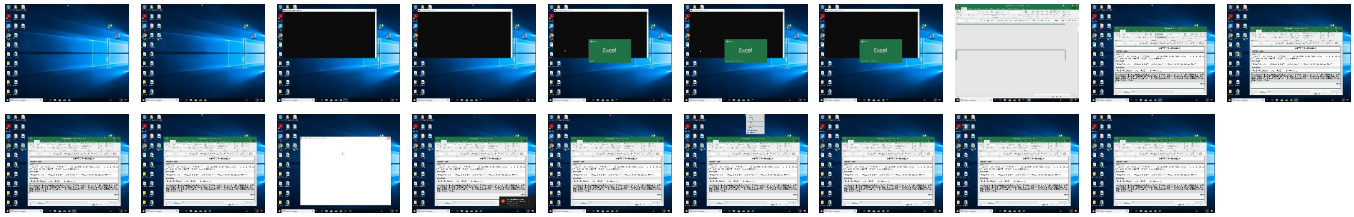
Behavior Graph

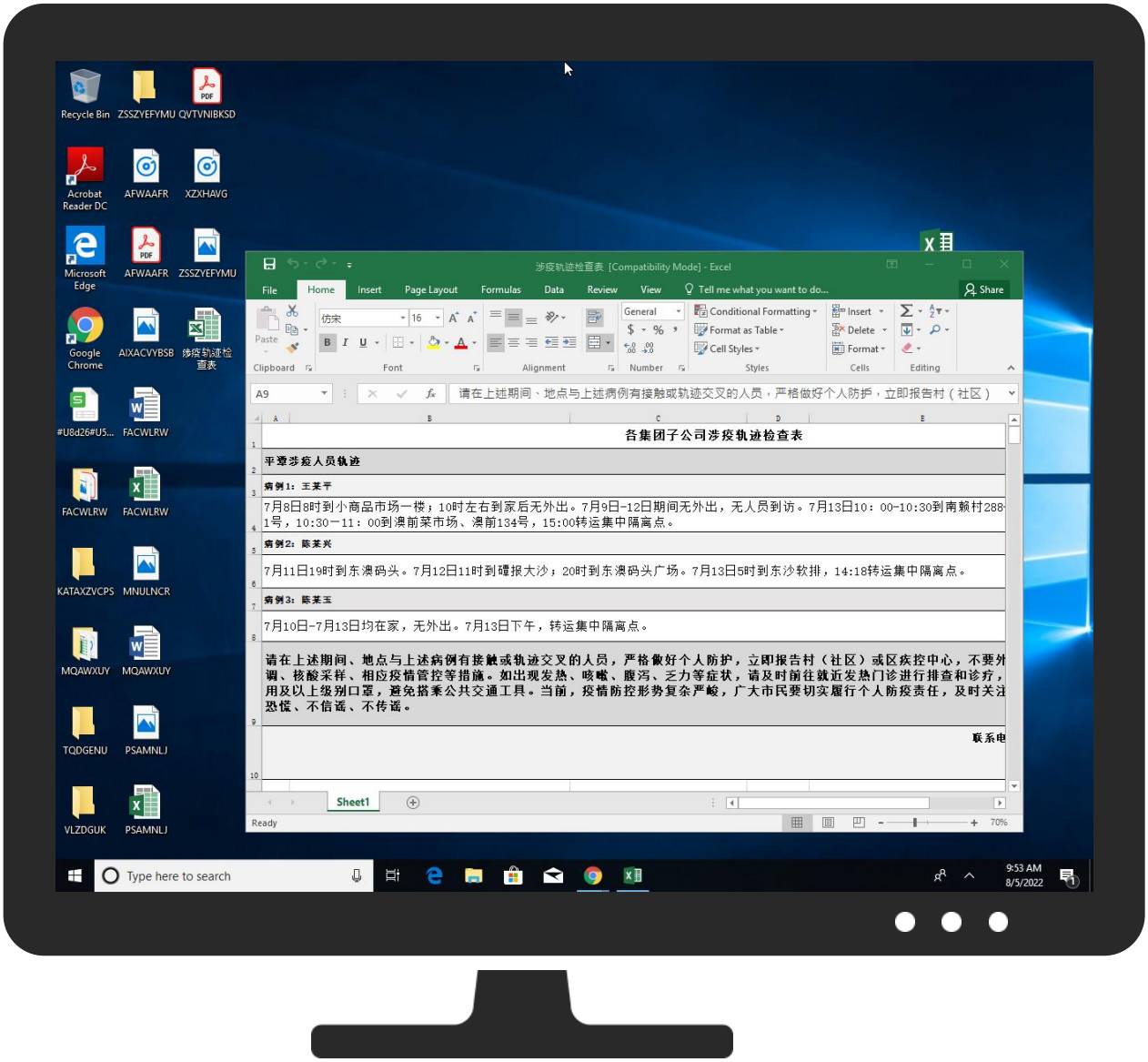


Screenshots

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
#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe	61%	Virustotal		Browse
#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe	26%	Metadefender		Browse
#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe	69%	ReversingLabs	Win64.Backdoor.CobaltStrikeBeacon	
#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe	100%	Avira	TR/Rozena.eozmy	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
jquery-min.us	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	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://cortana.ai	0%	URL Reputation	safe	
http://27.0.135.13/	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://jquery-min.us:8443/jquery-3.3.2.slim.min.jsL	0%	Avira URL Cloud	safe	
http://https://jquery-min.us:8443/	5%	Virustotal		Browse
http://https://jquery-min.us:8443/	0%	Avira URL Cloud	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://jquery-min.us:8443/jquery-3.3.2.slim.min.js	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	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://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.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://jquery-min.us:8443/s	0%	Avira URL Cloud	safe	
http://27.0.135.13/%E6%B6%89%E7%96%AB%E8%BD%A8%E8%BF%B9%E6%A3%80%E6%9F%A5%E8%A1%A8.xls	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://jquery-min.us:8443/jquery-3.3.2.slim.min.js	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	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
jquery-min.us	unknown	unknown	true	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://27.0.135.13/%E6%B6%89%E7%96%AB%E8%BD%A8%E8%BF%B9%E6%A3%80%E6%9F%A5%E8%A1%A8.xls	false	• Avira URL Cloud: safe	unknown
http://jquery-min.us:8443/jquery-3.3.2.slim.min.js	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://login.microsoftonline.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://shell.suite.office.com:1443	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://autodiscover-s.outlook.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://roaming.edog.	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://cdn.entity.	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://powerlift.acompli.net	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://cortana.ai	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://27.0.135.13/	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.aadrm.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://jquery-min.us:8443/jquery-3.3.2.slim.min.jsL	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe, 00000000.00000002.444303139.00000000000AC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://jquery-min.us:8443/	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe, 00000000.00000002.444391043.0000000000105000.00000004.00000020.00020000.00000000.sdmp, #U8d26#U53f7#U5bc6#U7801#U8868.xls.exe, 00000000.00000002.444431501.0000000000121000.00000004.00000020.00020000.00000000.sdmp	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://api.microsoftstream.com/api/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://cr.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://jquery-min.us:8443/jquery-3.3.2.slim.min.js	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe, 00000000.00000002.444303139.00000000000AC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://graph.ppe.windows.net	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://officeci.azurewebsites.net/api/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://my.microsoftpersonalcontent.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://globaldisco.crm.dynamics.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://messaging.engagement.office.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://dev0-api.acompli.net/autodetect	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://web.microsoftstream.com/video/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://dataservice.o365filtering.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://jquery-min.us:8443/s	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe, 00000000.00000002.444431501.000000000121000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://ncus.contentsync.	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://weather.service.msn.com/data.aspx	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://apis.live.net/v5.0/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://messaging.lifecycle.office.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://management.azure.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://outlook.office365.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://code.jquery.com/	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe, 00000000.00000002.444448493.000000000131000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://wus2.contentsync.	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://api.office.net	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://incidents.diagnosticssdf.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://entitlement.diagnostics.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://substrate.office.com/search/api/v2/init	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://outlook.office.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://outlook.office365.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://webshell.suite.office.com	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://management.azure.com/	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD.3.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
27.0.135.13	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679121
Start date and time: 05/08/202209:51:09	2022-08-05 09:51:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.evad.winEXE@7/4@10/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.7% (good quality ratio 74.3%) • Quality average: 53.9% • Quality standard deviation: 34.8%

HCA Information:	• Successful, ratio: 57% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 52.109.76.36, 52.109.88.37, 52.242.101.226, 52.152.110.14, 40.125.122.176
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, arc.msn.com, licensing.mp.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\B0F622F0-4ECB-4A62-9DE8-0BE100D4B6DD

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):	148061
Entropy (8bit):	5.358147023528658
Encrypted:	false
SSDEEP:	1536:PcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:O1Q9DQe+zuXYr
MD5:	FC031BF22CE6E9FCF3BBCD4645CC9CAA

SHA1:	3ECABDA5BEB7E8F758F225F03AF3E2FE32FADAD6
SHA-256:	542DAFFD4B4486F72BA534DA409FC90F7696E509FB24A87801778D045C792E4D
SHA-512:	AAE4BCF5B25CF638EE21FFCD481003D5157297DE8CFE7A81EA0FB20ADE9CC81FF296E8A63119FA9C4B12B959AB9D9E0E5B7B291DA18EFDDD4BE2AD40E31AC557
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="2022-08-05T07:52:31">.. Build: 16.0.15601.30525-->.. <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\Roaming\Microsoft\Office\Recent\???????.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=Fri Aug 5 15:52:21 2022, mtime=Fri Aug 5 15:52:32 2022, atime=Fri Aug 5 15:52:32 2022, length=23552, window=hide
Category:	dropped
Size (bytes):	1127
Entropy (8bit):	4.789260694079556
Encrypted:	false
SSDEEP:	12:8DsbhU9i6CHiLPNGX1Dwq+WAiucUy+o/ypa0Fb5b5Dyb0W4t2Y+xIBjKZm:8Dzopw0Oy+oKxJ5DyZ7aB6m
MD5:	3392F754CE250939539B340C618EE80F
SHA1:	96A237267FBD787C190689590FBD96EE1CAB8D3A
SHA-256:	0CB29152EEE395876B8ADB547B63CB737568A6F4471C9E8DFE25A8A55708FADA
SHA-512:	958ADCD9B0A49310864197CA38CE0D6E154A4B8E6CE4CD8DAFCB133DD815F82867B7CB2DA4ECF59B6677B89F9673C6091934D61B19E0C0303B1967BDDF04C47
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...w.....]..~....p.|.....\.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...U.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....hT....user..>.....NM..U.....S.....a.l.f.o.n.s.....~.1.....U....Desktop.h.....NM..U.....Y.....>.....U.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....b.2..\...U.. .839F~1.XLS..H.....U...U...../.....m.uh....h.gh...x.l.s.....$.....$...5.....Z.....>.S.....C:\Users\user\Desktop\???????.xls..C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.D.e.s.k.t.o.p.\..m.uh....h.gh...x.l.s.....".....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\..m.uh....h.gh...x.l.s.....:..,.LB.)...Aw..`.....X.....445817.....!a..%.H.VZAj.....s.....W...!a..%.H.VZAj.....s.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.

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:	modified
Size (bytes):	65
Entropy (8bit):	4.125194930303051
Encrypted:	false
SSDEEP:	3:bDuMJlWb6lmMCLb6lv:bCNsW0
MD5:	C542BE0A3F696F4BD179F109E96EA1EF
SHA1:	429D43CAA9F2FAB8F03016524B779816F71696B1
SHA-256:	F0B490700453792AB1B1C015A8CD5A55E0ED0B310DB560C8BCE2E7A0BEEF62B6
SHA-512:	2734D51FBDDB322C8FB605054AC112C4079A3998ADDCC3723C65B4BD7C5D4A4A6EF4497376BBBF70DD5009B0A8EAF8D811A3D1114E3DD6823DF134DF38E41A1
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..???????.LNK=0..[xls]..???????.LNK=0..

C:\Users\user\Desktop\???????.xls

Process:	C:\Users\user\Desktop\#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1200, Locale ID: 2052, Author: ma, Last Saved By: Adminis, Create Time/Date: Sun Jul 25 22:22:00 2021, Last Saved Time/Date: Mon Jul 18 16:11:36 2022, Name of Creating Application: WPS Of, Security: 0
Category:	dropped
Size (bytes):	23552
Entropy (8bit):	4.7469238649865835
Encrypted:	false
SSDEEP:	384:dCCCDQS4zTbleoPE8KI0fXb6HTsRQSO0JXGzfW6JjLuJj1zusAp7xOGz4uv8YXFh:dCCCDQS4zTbleoPE8KI0fXb0sGz4ud1G
MD5:	F5A8F916C2B8117DBF1CC1EA3319C8DA
SHA1:	B8E4B9E1247C54ED45BBA90CD2F1AAEDC0713372

SHA-256:	11E29E4983EAB5BBC95B11B06C8AD11A7375017B99B10FDE72F2669E5288E6BE
SHA-512:	05F5189A4F09A442D07D9440156B4F18C67284130D545C79CD701C72AF6A5B030DF1FD7C83F46D934749EB28AEF32936216AE4EB96D19129A5B3743B562F3DD8
Malicious:	false
Reputation:	low
Preview:	.....>.....(..... .....+..... ....!..".#...$...%...&..'.....*...,..... .....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.991293672325191
TrID:	• Win64 Executable (generic) (12005/4) 74.95% • Generic Win/DOS Executable (2004/3) 12.51% • DOS Executable Generic (2002/1) 12.50% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe
File size:	1553920
MD5:	2d2e2831ae6351fbee7810bfc0d10955
SHA1:	52a95894b8551743058a1bfe56e38919f43819c4
SHA256:	ffeb7d694c82c2dfa5344d082b61386561202ccde69fc11257916b0da515c922
SHA512:	239d6ad7b0654146b8c5c08a9b2f07a770cfb0ddabbbcad03109f82b0e78494f80097a98de7d55487f90f41ac25e09f028b12f60c5fc30863d1c871dfbff8eb5
SSDEEP:	24576:GW4sP/ippqFg0wSEn/v3KY1EoylYBAOL3jiVFToMK/GoFabCWx5h/xz1iWnmTlT:7xIqFPEH6YWooYBAOL3GVFTs/DFiCMNq
TLSH:	CB7533D17703E012D5B611702AA38B36556FFC2BEE38574AAF11BF2F1D317A68858A42
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....DL.....#..... .....09. TP..@9...@.....Q..... .....

File Icon

Icon Hash:	74e4c4e4c4d4c4c4

Static PE Info

General

Entrypoint:	0x905420
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	6ed4f5f04d62b18d96b26d6db7c18840

Entrypoint Preview

Instruction
push ebx
push esi

Instruction
push edi
push ebp
dec eax
lea esi, dword ptr [FFE8EBFAh]
dec eax
lea edi, dword ptr [esi-00393025h]
push edi
mov eax, 005034F4h
push eax
dec eax
mov ecx, esp
dec eax
mov edx, edi
dec eax
mov edi, esi
mov esi, 001713F4h
push ebp
dec eax
mov ebp, esp
inc esp
mov ecx, dword ptr [ecx]
dec ecx
mov eax, edx
dec eax
mov edx, esi
dec eax
lea esi, dword ptr [edi+02h]
push esi
mov al, byte ptr [edi]
dec edx
mov cl, al
and al, 07h
shr cl, 00000003h
dec eax
mov ebx, FFFFFD00h
dec eax
shl ebx, cl
mov cl, al
dec eax
lea ebx, dword ptr [esp+ebx*2-00000E78h]
dec eax
and ebx, FFFFFFC0h
push 00000000h
dec eax
cmp esp, ebx
jne 00007F1D1076980Bh
push ebx
dec eax
lea edi, dword ptr [ebx+08h]
mov cl, byte ptr [esi-01h]
dec edx
mov byte ptr [edi+02h], al
mov al, cl
shr cl, 00000004h
mov byte ptr [edi+01h], cl
and al, 0Fh
mov byte ptr [edi], al
dec eax
lea ecx, dword ptr [edi-04h]

Instruction
push eax
inc ecx
push edi
dec eax
lea eax, dword ptr [edi+04h]
inc ebp
xor edi, edi
inc ecx
push esi
inc ecx
mov esi, 00000001h
inc ecx
push ebp
inc ebp
xor ebp, ebp
inc ecx
push esp
push ebp
push ebx
dec eax
mov dword ptr [esp-10h], ecx
dec eax
mov dword ptr [esp-28h], eax
mov eax, 00000001h
dec eax
mov dword ptr [esp-08h], esi
dec esp
mov dword ptr [esp-18h], eax
mov ebx, eax
inc esp
mov dword ptr [esp-1Ch], ecx
movzx ecx, byte ptr [edi+02h]
shl ebx, cl
mov ecx, ebx
dec eax
mov ebx, dword ptr [esp+38h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x50f320	0x9c	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x506000	0x9320	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x393000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
UPX1	0x394000	0x172000	0x172000	False	0.9995077597128378	data	7.99986627038318	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x506000	0xa000	0x9400	False	0.43911000844594594	data	5.674111167289192	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5062e4	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x506410	0x2e8	data	English	United States
RT_ICON	0x5066fc	0x668	dBase IV DBT of `.DBF, block length 1536, next free block index 40, next free block 248, next used block 65280	English	United States
RT_ICON	0x506d68	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x5072d4	0x8a8	data	English	United States
RT_ICON	0x507b80	0xea8	data	English	United States
RT_ICON	0x508a2c	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x508e98	0x10a8	data	English	United States
RT_ICON	0x509f44	0x25a8	data	English	United States
RT_ICON	0x50c4f0	0x2885	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_GROUP_ICON	0x50ed7c	0x92	data	English	United States
RT_VERSION	0x50ee14	0x300	data	English	United States
RT_MANIFEST	0x50f118	0x207	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.DLL	LoadLibraryA, ExitProcess, GetProcAddress, VirtualProtect

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 23

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:52:21.419822931 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:24.538278103 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:24.785228968 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:24.785429955 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:24.789292097 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:25.036046982 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036730051 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036756992 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036781073 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036819935 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036844969 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036866903 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036870003 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:25.036890030 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036912918 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036921978 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:25.036936998 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036961079 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.036973953 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:25.037055969 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:25.283895969 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.283956051 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.283998013 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.284045935 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.284099102 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.284156084 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.284203053 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.284224033 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:25.284257889 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:25.284290075 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:25.284334898 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:30.042006969 CEST	80	49737	27.0.135.13	192.168.2.5
Aug 5, 2022 09:52:30.042123079 CEST	49737	80	192.168.2.5	27.0.135.13
Aug 5, 2022 09:52:31.032546043 CEST	49737	80	192.168.2.5	27.0.135.13

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:52:27.284778118 CEST	53821	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:27.340873003 CEST	53	53821	8.8.8.8	192.168.2.5
Aug 5, 2022 09:52:27.376110077 CEST	61356	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:27.434125900 CEST	53	61356	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:52:27.453694105 CEST	59661	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:27.511209011 CEST	53	59661	8.8.8.8	192.168.2.5
Aug 5, 2022 09:52:27.543205976 CEST	57278	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:27.595329046 CEST	53	57278	8.8.8.8	192.168.2.5
Aug 5, 2022 09:52:27.624944925 CEST	53757	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:27.682616949 CEST	53	53757	8.8.8.8	192.168.2.5
Aug 5, 2022 09:52:27.720825911 CEST	54322	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:27.782706022 CEST	53	54322	8.8.8.8	192.168.2.5
Aug 5, 2022 09:52:27.831644058 CEST	62704	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:27.885870934 CEST	53	62704	8.8.8.8	192.168.2.5
Aug 5, 2022 09:52:27.958754063 CEST	53934	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:28.013510942 CEST	53	53934	8.8.8.8	192.168.2.5
Aug 5, 2022 09:52:28.044615984 CEST	63712	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:28.100229979 CEST	53	63712	8.8.8.8	192.168.2.5
Aug 5, 2022 09:52:28.113236904 CEST	63187	53	192.168.2.5	8.8.8.8
Aug 5, 2022 09:52:28.165755033 CEST	53	63187	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 09:52:27.284778118 CEST	192.168.2.5	8.8.8.8	0xbe52	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.376110077 CEST	192.168.2.5	8.8.8.8	0x6f97	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.453694105 CEST	192.168.2.5	8.8.8.8	0xe9b3	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.543205976 CEST	192.168.2.5	8.8.8.8	0xae71	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.624944925 CEST	192.168.2.5	8.8.8.8	0xbbaa	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.720825911 CEST	192.168.2.5	8.8.8.8	0x4118	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.831644058 CEST	192.168.2.5	8.8.8.8	0x8553	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.958754063 CEST	192.168.2.5	8.8.8.8	0x9791	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:28.044615984 CEST	192.168.2.5	8.8.8.8	0x8928	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:28.113236904 CEST	192.168.2.5	8.8.8.8	0x7bd3	Standard query (0)	jquery-min.us	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 09:52:27.340873003 CEST	8.8.8.8	192.168.2.5	0xbe52	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.434125900 CEST	8.8.8.8	192.168.2.5	0x6f97	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.511209011 CEST	8.8.8.8	192.168.2.5	0xe9b3	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.595329046 CEST	8.8.8.8	192.168.2.5	0xae71	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.682616949 CEST	8.8.8.8	192.168.2.5	0xbbaa	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.782706022 CEST	8.8.8.8	192.168.2.5	0x4118	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:27.885870934 CEST	8.8.8.8	192.168.2.5	0x8553	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:28.013510942 CEST	8.8.8.8	192.168.2.5	0x9791	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:28.100229979 CEST	8.8.8.8	192.168.2.5	0x8928	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)
Aug 5, 2022 09:52:28.165755033 CEST	8.8.8.8	192.168.2.5	0x7bd3	Server failure (2)	jquery-min.us	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 27.0.135.13

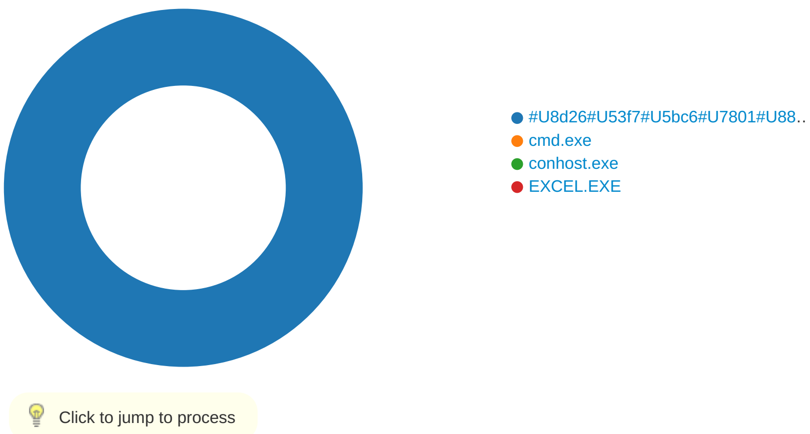
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49737	27.0.135.13	80	C:\Users\user\Desktop\#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 09:52:24.789292097 CEST	456	OUT	GET /%E6%B6%89%E7%96%AB%E8%BD%A8%E8%BF%B9%E6%A3%80%E6%9F%A5%E8%A1%A8.xls HTTP/1.1 Host: 27.0.135.13 User-Agent: Go-http-client/1.1 Accept-Encoding: gzip
Aug 5, 2022 09:52:25.036730051 CEST	458	IN	HTTP/1.1 200 OK Date: Fri, 05 Aug 2022 07:52:24 GMT Server: Apache/2.4.6 (CentOS) Last-Modified: Mon, 18 Jul 2022 15:13:28 GMT ETag: "5c00-5e415cf643743" Accept-Ranges: bytes Content-Length: 23552 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 01 00 00 00 01 00 00 00 00 00 00 00 00 10 00 00 28 00 00 00 01 00 00 00 fe ff ff ff 00 00 00 00 00 00 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 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 2b 00 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 fe ff ff ff fe ff ff ff 2a 00 00 00 2c 00 00 00 fe ff ff ff fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16 00 05 00 Data Ascii: >(+ !"#$%&'*,Root Entry

Statistics

Behavior



System Behavior

Analysis Process: #U8d26#U53f7#U5bc6#U7801#U8868.xls.exe PID: **5940**, Parent PID: **5688**

General

Target ID:	0
Start time:	09:52:20
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\#U8d26#U53f7#U5bc6#U7801#U8868.xls.exe"
Imagebase:	0x400000
File size:	1553920 bytes
MD5 hash:	2D2E2831AE6351FBEE7810BFC0D10955
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Cobaltbaltstrike_RAW_Payload_https_stager_x64, Description: Detects CobaltStrike payloads, Source: 00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike, Description: Yara detected CobaltStrike, Source: 00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Metasploit_7bc0f998, Description: Identifies the API address lookup function leverage by metasploit shellcode, Source: 00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Metasploit_c9773203, Description: Identifies the 64 bit API hashing function used by Metasploit. This has been re-used by many other malware families., Source: 00000000.00000002.449971931.000000C0001CE000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000000.00000002.450050616.000000C0001D4000.00000004.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_CobaltStrike, Description: Yara detected CobaltStrike, Source: 00000000.00000002.450050616.000000C0001D4000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Cobaltbaltstrike_RAW_Payload_https_stager_x64, Description: Detects CobaltStrike payloads, Source: 00000000.00000002.447338281.0000000026E30000.00000040.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000000.00000002.447338281.0000000026E30000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Metasploit_7bc0f998, Description: Identifies the API address lookup function leverage by metasploit shellcode, Source: 00000000.00000002.447338281.0000000026E30000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Metasploit_c9773203, Description: Identifies the 64 bit API hashing function used by Metasploit. This has been re-used by many other malware families., Source: 00000000.00000002.447338281.0000000026E30000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: **5828**, Parent PID: **5940**

General

Target ID:	1
Start time:	09:52:25
Start date:	05/08/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\cmd.exe /C start ???????.xls
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: conhost.exe PID: **4540**, Parent PID: **5828**

General

Target ID:	2
Start time:	09:52:25
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: EXCEL.EXE PID: **5232**, Parent PID: **5828**

General

Target ID:	3
Start time:	09:52:29
Start date:	05/08/2022
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:	0xfc0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly