ID: 632999
Sample Name: e5#U7248.exe
Cookbook: default.jbs
Time: 11:17:13
Date: 24/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

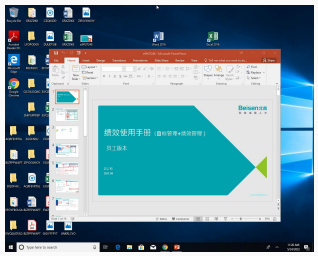
Windows Analysis Report

e5#U7248.exe

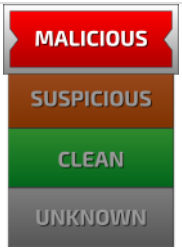
Overview

General Information

Sample Name:	e5#U7248.exe
Analysis ID:	632999
MD5:	032e7e721dfe5d..
SHA1:	4a214becd642f2..
SHA256:	dac35a874ca47b..
Tags:	CobaltStrike exe
Infos:	



Detection



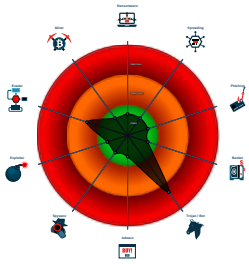
CobaltStrike

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected CobaltStrike
- Self deletion via cmd delete
- Deletes itself after installation
- C2 URLs / IPs found in malware con…
- Yara signature match
- Uses code obfuscation techniques (…
- Sample execution stops while proce…
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files

Classification



Process Tree

- **System is w10x64**
- e5#U7248.exe (PID: 7116 cmdline: "C:\Users\user\Desktop\e5#U7248.exe" MD5: 032E7E721DFE5DBC95BB91A3BC2E935C)
  - POWERPNT.EXE (PID: 3256 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE" "C:\Users\user\Desktop\e5#U7248.pptx" /ou " MD5: 68F52CD14C61DDC941769B55AE3F2EE9)
  - e5#U7248.exe (PID: 6884 cmdline: C:\Users\Public\Music\e5#U7248.exe MD5: 032E7E721DFE5DBC95BB91A3BC2E935C)
  - cmd.exe (PID: 820 cmdline: "C:\Windows\system32\cmd.exe" /c del C:\Users\user\Desktop\e5#U7248.exe > nul MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: CobaltStrike


```
{
  "C2Server": "http://service-ep07djah-1306669097.bj.apigw.tencentcs.com:443/bootstrap-2.min.js",
  "User Agent": "User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)\r\n"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.631477810.000001C8CA0EB000.00000004.00000020.00020000.00000000.sdmp	Cobaltbaltstrike_RAW_Payload_https_stager_x64	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x6fb0:$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
0000000C.00000002.631477810.000001C8CA0EB000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CobaltStrike_3	Yara detected CobaltStrike	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.631567397.000001C8CA290000.00000040.00001000.00020000.00000000.sdmp	CobaltbaltstrikeRAW_Payload_https_stager_x64	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x0:$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
0000000C.00000002.631567397.000001C8CA290000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_CobaltStrike_3	Yara detected CobaltStrike	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Deletes itself after installation

Remote Access Functionality

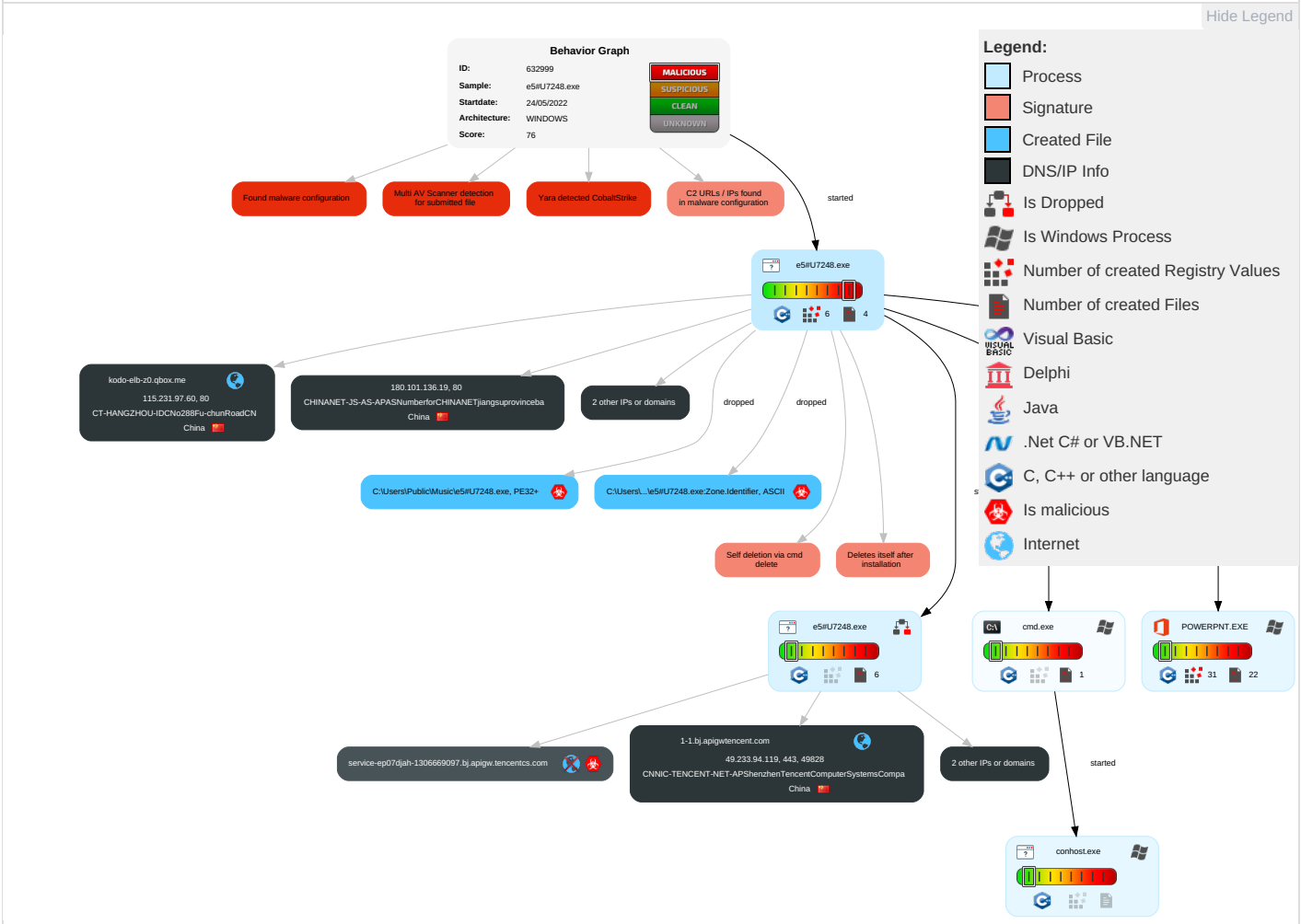
Yara detected CobaltStrike

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 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 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 Query Registry	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Extra Window Memory Injection	2 Obfuscated Files or Information	Security Account Manager	1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 2 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 Software Packing	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 File Deletion	Cached Domain Credentials	3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Extra Window Memory Injection	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

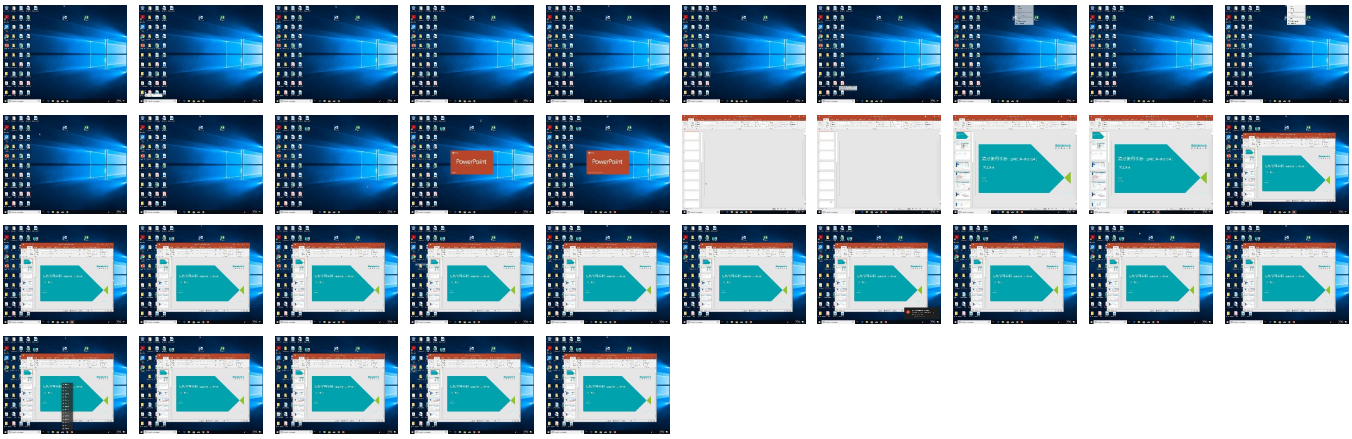
Behavior Graph

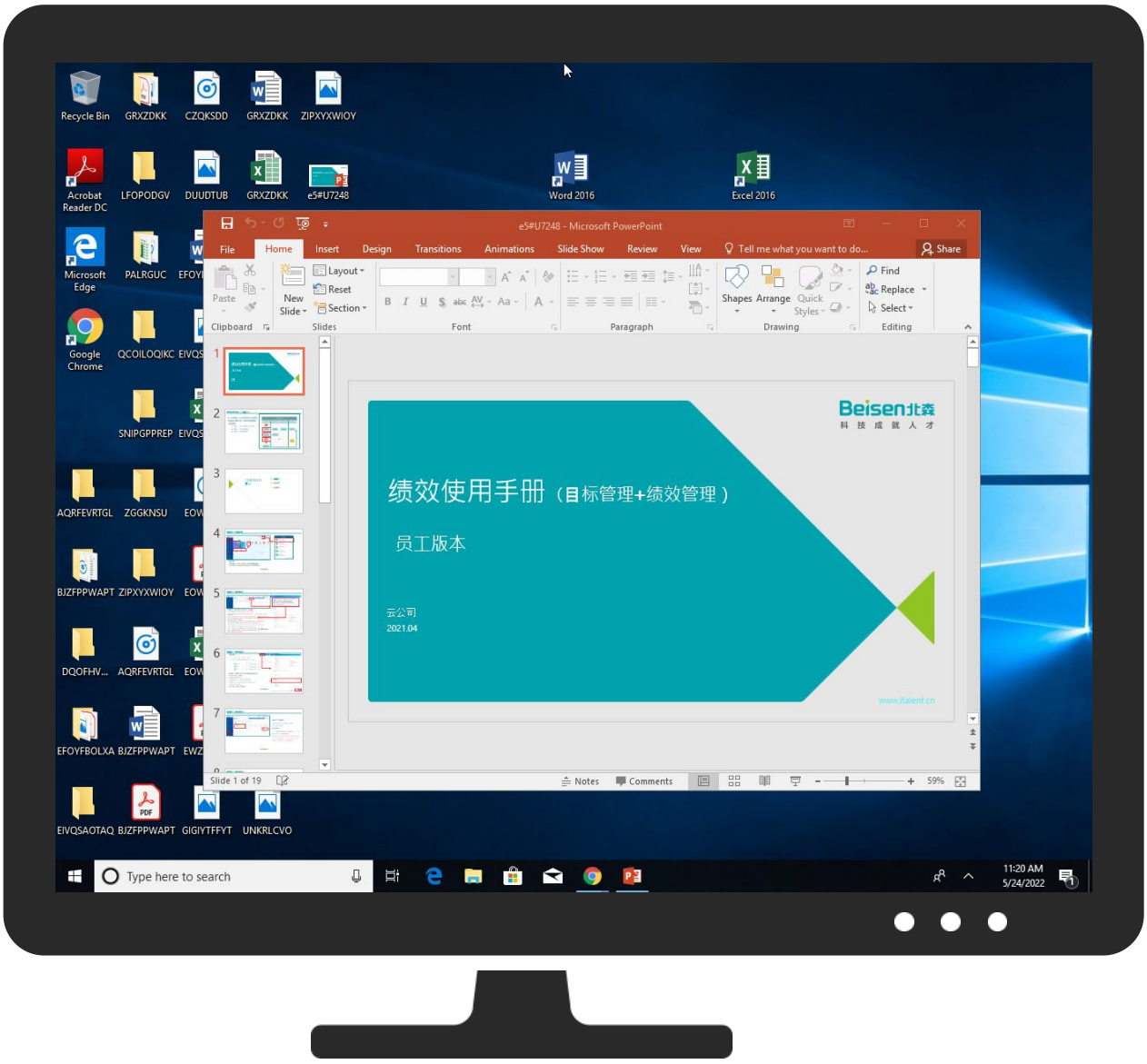


Screenshots

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
e5#U7248.exe	9%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
service-ep07djah-1306669097.bj.apigw.tencentcs.com	0%	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://rs.qbox.mehttp://rsf.qbox.mehttp://api.qiniu.comhttp://fusion.qiniuapi.comhttp://uc.qbox.meht	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://curl.se/docs/hsts.html	0%	Avira URL Cloud	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.js	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://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://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.jsT	0%	Avira URL Cloud	safe	
http://upload.qiniup.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://curl.se/docs/alt-svc.html	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://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://fusion.qiniuapi.com	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://service-ep07djah-1306669097.bj.apigw.tencentcs.com:443/bootstrap-2.min.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
1-1.bj.apigwtencent.com	49.233.94.119	true	false		unknown
kodo-elb-z0.qbox.me	115.231.97.60	true	false		high
service-ep07djah-1306669097.bj.apigw.tencentcs.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
rs.qbox.me	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://service-ep07djah-1306669097.bj.apigw.tencentcs.com:443/bootstrap-2.min.js	true	• Avira URL Cloud: safe	unknown

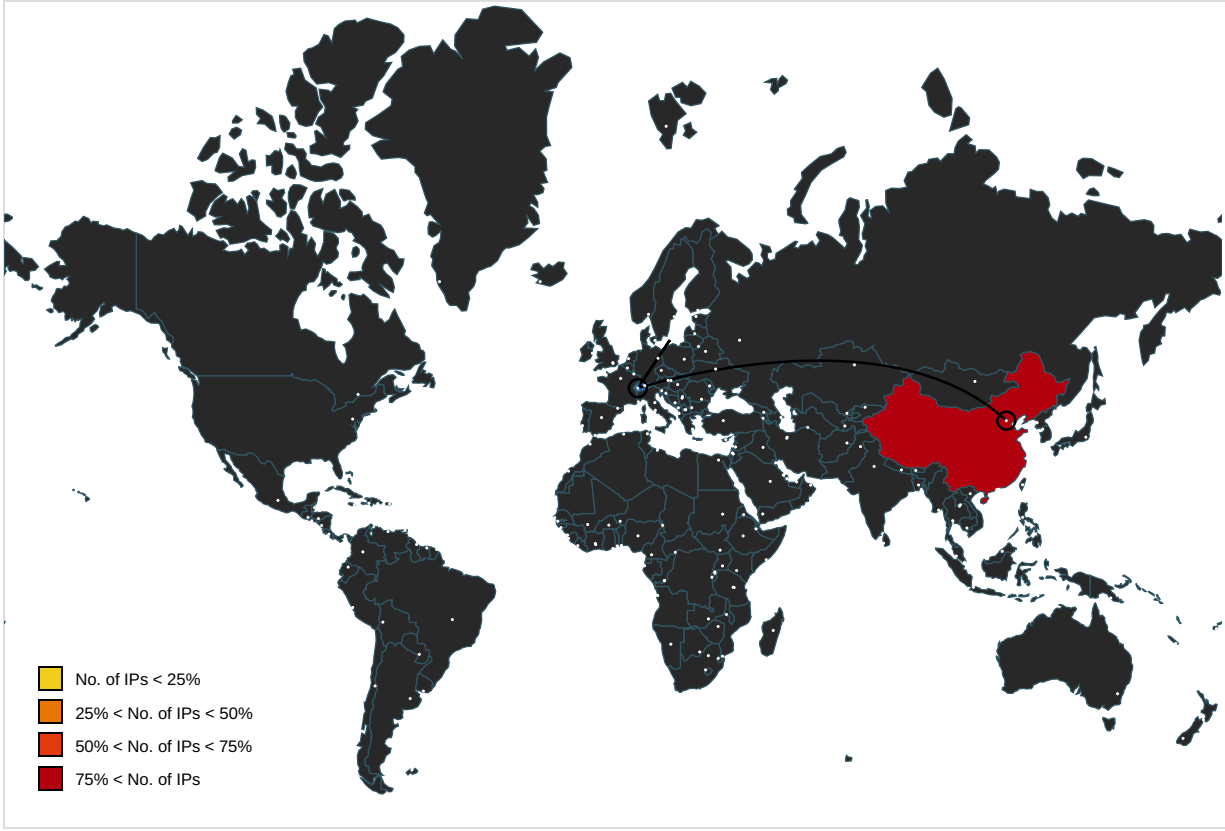
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://login.microsoftonline.com/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://shell.suite.office.com:1443	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://rs.qbox.me/chtype/RGJhay9jaGRiOnFpbml1LnBuZw==/type/1	e5#U7248.exe, 0000000C.00000002.63143157 0.000001C8CA0A8000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://autodiscover-s.outlook.com/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://roaming.edog.	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://cdn.entity.	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://powerlift.acompli.net	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://api.qiniu.com	e5#U7248.exe, e5#U7248.exe.1.dr	false		high
http://https://cortana.ai	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://rs.qbox.mehttp://rsf.qbox.mehttp://api.qiniu.comhttp://fusion.qiniuapi.comhttp://uc.qbox.meht	e5#U7248.exe, e5#U7248.exe.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.onenote.com/upload.aspx	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://api.aadrm.com/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://rs.qbox.me/chtype/RGJhay9jaGRiOnFpbml1LnBuZw==/type/1da	e5#U7248.exe, 00000001.00000002.53400482 8.00000150D073B000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://curl.se/docs/hsts.html	e5#U7248.exe, e5#U7248.exe.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.js	e5#U7248.exe, 0000000C.00000002.63147781 0.000001C8CA0EB000.00000004.00000020.000 20000.00000000.sdmp, e5#U7248.exe, 00000 00C.00000002.631506915.000001C8CA111000. 00000004.00000020.00020000.00000000.sdmp, e5#U7248.exe, 0000000C.00000002.631431 570.000001C8CA0A8000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://api.microsoftstream.com/api/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://cr.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://graph.ppe.windows.net	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://officeci.azurewebsites.net/api/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.jsT	e5#U7248.exe, 0000000C.00000002.63147781 0.000001C8CA0EB000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://upload.qiniup.com	e5#U7248.exe, e5#U7248.exe.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://globaldisco.crm.dynamics.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://messaging.engagement.office.com/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://dev0-api.acompli.net/autodetect	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://web.microsoftstream.com/video/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://curl.se/docs/alt-svc.html	e5#U7248.exe, e5#U7248.exe.1.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://dataservice.o365filtering.com/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://ncus.contentsync.	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://weather.service.msn.com/data.aspx	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://apis.live.net/v5.0/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://management.azure.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://outlook.office365.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://wus2.contentsync.	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://iovip.qbox.me	e5#U7248.exe, e5#U7248.exe.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://api.office.net	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://incidents.diagnosticssdf.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://fusion.qiniuapi.com	e5#U7248.exe, e5#U7248.exe.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://asgsmsproxyapi.azurewebsites.net/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://entitlement.diagnostics.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://rs.qbox.me/chtype/RGJhay9jaGRiOnFpbml1LnBuZw==/type/1-1000	e5#U7248.exe, 00000001.00000002.534004828.00000150D073B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://substrate.office.com/search/api/v2/init	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://outlook.office.com/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://outlook.office365.com/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://webshell.suite.office.com	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://rsf.qbox.me	e5#U7248.exe, e5#U7248.exe.1.dr	false		high
http://https://management.azure.com/	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	335F8B80-9649-4ACE-A711-42A021E2413D.11.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
115.231.97.60	kodo-elb-z0.qbox.me	China		58461	CT-HANGZHOU-IDCNo288Fu-chunRoadCN	false
49.233.94.119	1-1.bj.apigwtencent.com	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
180.101.136.19	unknown	China		23650	CHINANET-JS-AS-APASNumberforCHINANETjiangsuprovinceba	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632999
Start date and time: 24/05/202211:17:13	2022-05-24 11:17:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e5#U7248.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:	24
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:	mal76.troj.winEXE@8/6@3/4
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 44.4% (good quality ratio 22.2%) • Quality average: 50% • Quality standard deviation: 50%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.109.88.177, 52.109.88.38, 52.109.88.40
- 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, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Execution Graph export aborted for target e5#U7248.exe, PID 7116 because there are no executed function
- Not all processes where analyzed, report is 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.
- Report size getting too big, too many NtSetInformationFile 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\Public\Music\e5#U7248.exe

Process:	C:\Users\user\Desktop\e5#U7248.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4937216
Entropy (8bit):	7.3137520514707
Encrypted:	false
SSDEEP:	98304:E0+E9G0lv7XF4UNcQV1wyw6qjw4y6UlDY2l:RX9G0lv714Q8Ux6U
MD5:	032E7E721DFE5DBC95BB91A3BC2E935C
SHA1:	4A214BECD642F2BF8DF0C118056A217AEC073CC5
SHA-256:	DAC35A874CA47B8DE8103AC84B2DB9DEA4E6B44F9ED2081FCD5BFF1143A66D97
SHA-512:	B0BEAC870FFBBD7F1B3DCB0586CFF81E543350EC97989A20D87029CEB279D089D80A54EF0F96A390334A45907AE0BF256B9CDBCDE5863A48D23DEEBE1E1B8E4D
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....~r...:y.:.y.:.y._u}...y._uz.6.y._u|...y.:.y.&.y.....=.y.h{z.3.y..z}.J.y._ux.5.y.:.x...y.h{|...y.h{}...y..z|.;.y..z..;.y.:...;.y..z{.;.y.Rich:.y.....PE..d....].b.....".....d...>.....@.....K.....`.....Z'.....@).HD"...(..$.....K.@]....&.....&.....text...$c.....d..... ..`.rdata.....h.....@..@.data.....'..2...Z'.....@....pdata...$....(..&...'.....@..@.rsrc...HD"..@)..F"...(.....@..@.reloc..@]....K..^....J.....@..B.....

C:\Users\Public\Music\e5#U7248.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\e5#U7248.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\335F8B80-9649-4ACE-A711-42A021E2413D

Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	147614
Entropy (8bit):	5.359221740812186
Encrypted:	false
SSDEEP:	1536:dcQk/gxgB5B3guw//Q9DQW+zQWk4F77nXmvidQXxFETLKz6e:jHQ9DQW+zIXQI
MD5:	774458080C9198580CF712EE05A4402E
SHA1:	6FBF80AA9C0E9545AB55F1BEB4AB264827DBBFFC
SHA-256:	DD90BA7F848AE754FDEB057DDBE8052F22A5E724E63E5958B8F2FAA7F503579F
SHA-512:	F4ACD6CFC1A33E4F6D2C7BF6248BEC83608621EB665A2F8A8CE1FC7A337ECE74FE322D665481C4C515F06CFAC2AE6B7F1C7706545D42C94E09A7195B5DBFDACE
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="2022-05-24T09:19:11">.. Build: 16.0.15315.30526-->.. <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\e5.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue May 24 17:19:07 2022, mtime=Tue May 24 17:19:12 2022, atime=Tue May 24 17:19:07 2022, length=2068461, window=hide
Category:	dropped
Size (bytes):	1063
Entropy (8bit):	4.707408336825349
Encrypted:	false
SSDEEP:	12:8Z6n19UkWCHo/XsImI+W3actKZijAk/E2m8NySOND8aLbzebzWk44t2Y+xIBjKZm:8ZIPetbAk8kuD3l7aB6m
MD5:	F1BDBB6BC6FDA893D1201A16F5DE6350
SHA1:	51C2BCB3410F422FAF14B6B821EE2A061BD7C9F7
SHA-256:	0A2B16A79A1FC75931BCD7EAC920924D365108F78A317E6011332F930338CDBA
SHA-512:	C3B859615A8047F09D96EBD6A7C15A1EF52CA9BED6F2F31491B6A5DA955D500AF475CE1C269665191F0A5D5C2AAF68C117CD50F5FAA84AB3DBE34CB95AC37BAC
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...O....o..5..o...3..o.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...TL.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....hTz...user..B.....N...TL.....S.....e.n.g.i.n.e.e.r.....~.1.....Td...Desktop.h.....N...Te.....Y.....>...../.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....h.2.....Td. .E5#U72~1.PPT..L.....Td..Td.....N.....P...e.5.#.U.7.2.4.8...p.p.t.x.....V.....-.....U.....>.S.....C:\Users\user\Desktop\e5#U7248.pptx..$....\....\....\....\....\.D.e.s.k.t.o.p.\.e.5.#.U.7.2.4.8...p.p.t.x.....:.,.LB.)...A}...`.....X.....210979.....!a..%.H.VZAj...s.>].....-$..!a..%.H.VZAj...s.>].....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	39
Entropy (8bit):	4.24040510342216
Encrypted:	false
SSDEEP:	3:HLeUm4Wv:HL6
MD5:	CC052D09B391D0854B3541F4821426BE
SHA1:	5C136CE22F57501A7DBCD9DFD01E908C15248C98
SHA-256:	53CABBF3DD7F4576F525C5B43A7A6BEC7A00CA1F7DF21CD33502EFB59090BEBA
SHA-512:	EB514552C627DA42B1E6420FB0C21E34C6E2BD8141ECAB7C9634B3A3BCE3AE2439C21662DB4A8752FE2F5DBED83779633833F6AD9887EA5A6C3CFDB95A270024
Malicious:	false
Reputation:	low
Preview:	[misc]..e5.LNK=0..[folders]..e5.LNK=0..

C:\Users\user\Desktop\e5#U7248.pptx	
Process:	C:\Users\user\Desktop\e5#U7248.exe
File Type:	Microsoft PowerPoint 2007+
Category:	modified
Size (bytes):	2068461
Entropy (8bit):	7.8112893691004865
Encrypted:	false
SSDEEP:	49152:uVFtwyfYBMRhxUjw4yTO6yLYO19JKLlooTYF8pl0:u1wyw6qjw4y6UlDY2l0
MD5:	3BBBC2FD0ACA510B778DE111409A3047
SHA1:	670F28428DAD6ACB57093F7A8C1D04DED167CBD1
SHA-256:	8E1F4B3779DC4DF4F7BF624AF91C4ABA042100651A6F2D41081F90BA3664463A
SHA-512:	FA80EFA24E920C89DBFC6107F21665C99AD997A44F96F93F127AEB742527F9CD72771A0192DE4E4647D8E5C074075B4B728B14861891073E7B4ECDB2ACAE9D47
Malicious:	false
Preview:	PK.....!.. H.c...T.....[Content_Types].xml ...(.....]o. ...'.?X.N1...n..}\.R.....5.~.NZ.rj....(..{.d...yvuW.d..0)2D.)J@.`b.._._'.(1...r) C[0.j....v..$.Z....U.16..JjR.@....%.n..X../].>.N.q...a'..@..gX.5..;w.!Qb..O.*U.XY.W.qg....!.Dw..n..P.8.u.x#.G{.....z.Y1e..G2T3....~...Y..5...-.*...J.qq...i..T.X.....K....J~0LK..~..`.w..Sc.ai...d-.AL;.0..!8.N.6:.....G'..Np...Ct.2.....I[[$.}..7F...I|k$..7G.....`.5dk0.K....V...k..:...u..GV.^k.L....#.0....^......_..Q..f..9..-.

Static File Info

General

File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	7.3137520514707
TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	e5#U7248.exe
File size:	4937216
MD5:	032e7e721dfe5dbc95bb91a3bc2e935c
SHA1:	4a214becd642f2bf8df0c118056a217aec073cc5
SHA256:	dac35a874ca47b8de8103ac84b2db9dea4e6b44f9ed2081fcd5bff1143a66d97
SHA512:	b0beac870ffbbd7f1b3dcb0586cff81e543350ec97989a20d87029ceb279d089d80a54ef0f96a390334a45907ae0bf256b9cdbcde5863a48d23deebe1e1b8e4d
SSDEEP:	98304:E0+E9G0Iv7XF4UNcQV1wyw6qjw4y6UlDY2l:RX9G0Iv714Q8Ux6U
TLSH:	2536DF1AAAA508E4DCB6C23886565633E7B1BC15277167EB03E0F6771F33AD11E3A704
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....~r..:.y.:.y.:.y._u}...y._uz.6.y._u|...y.::y.&.y.....=.y.h{z.3.y..z}.J.y._ux.5.y.:.x...y.h{|...y.h{}...y..z|.;.y..z..;.y.:...;.y

File Icon

Icon Hash:	30868c8c8c868830

Static PE Info

General

Entrypoint:	0x14007c5bc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x628B5D9D [Mon May 23 10:10:37 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	62a5dd25af85564e3aeb55c6407225e3

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
call 00007F49B89ACA30h
dec eax
add esp, 28h
jmp 00007F49B89ABFBFh
int3
int3
inc eax
push ebx
dec eax

Instruction
sub esp, 20h
dec eax
mov ebx, ecx
jmp 00007F49B89AC151h
dec eax
mov ecx, ebx
call 00007F49B8A93A2Ah
test eax, eax
je 00007F49B89AC155h
dec eax
mov ecx, ebx
call 00007F49B8A8675Ah
dec eax
test eax, eax
je 00007F49B89AC129h
dec eax
add esp, 20h
pop ebx
ret
dec eax
cmp ebx, FFFFFFFFh
je 00007F49B89AC148h
call 00007F49B89ACDF8h
int3
call 00007F49B89ACE12h
int3
jmp 00007F49B89ACE2Ch
int3
int3
int3
jmp 00007F49B89AC0FCh
int3
int3
int3
dec eax
sub esp, 28h
dec ebp
mov eax, dword ptr [ecx+38h]
dec eax
mov ecx, edx
dec ecx
mov edx, ecx
call 00007F49B89AC152h
mov eax, 00000001h
dec eax
add esp, 28h
ret
int3
int3
int3
inc eax
push ebx
inc ebp
mov ebx, dword ptr [eax]
dec eax
mov ebx, edx
inc ecx
and ebx, FFFFFFF8h
dec esp

Instruction
mov ecx, ecx
inc ecx
test byte ptr [eax], 00000004h
dec esp
mov edx, ecx
je 00007F49B89AC155h
inc ecx
mov eax, dword ptr [eax+08h]
dec ebp
arpl word ptr [eax+04h], dx
neg eax
dec esp
add edx, ecx
dec eax
arpl ax, cx
dec esp
and edx, ecx
dec ecx
arpl bx, ax
dec edx
mov edx, dword ptr [eax+edx]
dec eax
mov eax, dword ptr [ebx+10h]
mov ecx, dword ptr [eax+08h]
dec eax
mov eax, dword ptr [ebx+08h]
test byte ptr [ecx+eax+03h], 0000000Fh
je 00007F49B89AC14Dh
movzx eax, byte ptr [ecx+eax+00h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x275a04	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x294000	0x224448	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x281000	0x12498	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4b9000	0x5d40	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x261b80	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x261ba0	0x100	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1d8000	0x710	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1d6324	0x1d6400	False	0.528704499767	data	6.83933595182	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1d8000	0x9f0d4	0x9f200	False	0.43268699676	data	5.72254467214	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x278000	0x81b0	0x3200	False	0.236875	DOS executable (block device driver ght (c)	3.22425146815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.pdata	0x281000	0x12498	0x12600	False	0.487417623299	data	6.1747245461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x294000	0x224448	0x224600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4b9000	0x5d40	0x5e00	False	0.264710771277	data	5.44086201759	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
FILE_DATA	0x2bc080	0x1f8fed	Microsoft PowerPoint 2007+	Chinese	China
FILE_DATA	0x4b5070	0x31aa	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 285x180, frames 3	Chinese	China
RT_ICON	0x2944b0	0x2e8	data	Chinese	China
RT_ICON	0x294798	0x128	GLS_BINARY_LSB_FIRST	Chinese	China
RT_ICON	0x2948c0	0x1628	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x295ee8	0xea8	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x296d90	0x8a8	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x297638	0x568	GLS_BINARY_LSB_FIRST	Chinese	China
RT_ICON	0x297ba0	0x10ef	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	Chinese	China
RT_ICON	0x298c90	0x94a8	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x2a2138	0x67e8	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x2a8920	0x5488	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x2adda8	0x4228	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x2b1fd0	0x3a48	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x2b5a18	0x25a8	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x2b7fc0	0x1a68	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x2b9a28	0x10a8	dBase III DBT, version number 0, next free block index 40	Chinese	China
RT_ICON	0x2baad0	0x988	data	Chinese	China
RT_ICON	0x2bb458	0x6b8	data	Chinese	China
RT_ICON	0x2bbb10	0x468	GLS_BINARY_LSB_FIRST	Chinese	China
RT_GROUP_ICON	0x2bbf78	0x102	data	Chinese	China
RT_MANIFEST	0x4b8220	0x224	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

DLL	Import
SHELL32.dll	SHGetSpecialFolderPathA, ShellExecuteExW, SHChangeNotify, ShellExecuteA
USER32.dll	SendMessageW, GetProcessWindowStation, GetUserObjectInformationW, MessageBoxW, LoadIconW

DLL	Import
KERNEL32.dll	TlsSetValue, TlsFree, GetSystemTimeAsFileTime, GetTickCount, GetModuleHandleW, GetProcAddress, CompareStringW, LCMapStringW, GetLocaleInfoW, GetStringTypeW, GetCPInfo, CreateFileA, GetFileInformationByHandle, ReadFile, CloseHandle, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleExW, GetStdHandle, GetFileType, WriteFile, DeleteFiber, ConvertFiberToThread, FreeLibrary, LoadLibraryA, LoadLibraryW, FindClose, FindFirstFileW, FindNextFileW, GetConsoleMode, SetConsoleMode, TlsGetValue, ReadConsoleW, GetDriveTypeW, CreateThread, RtlUnwind, VerifyVersionInfoW, VerSetConditionMask, WaitForMultipleObjects, GetEnvironmentVariableA, WaitForSingleObjectEx, MoveFileExA, GetModuleHandleA, GetSystemDirectoryA, QueryPerformanceFrequency, SleepEx, Sleep, InitializeCriticalSectionEx, SetEndOfFile, WriteConsoleW, HeapSize, GetFullPathNameW, GetCurrentDirectoryW, GetProcessHeap, SetStdHandle, SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetCommandLineA, GetOEMCP, GetACP, CreateFileW, IsValidCodePage, FindFirstFileExW, GetTimeZoneInformation, HeapReAlloc, SetFilePointerEx, GetFileSizeEx, GetConsoleCP, FlushFileBuffers, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, GetTimeFormatW, GetDateFormatW, HeapAlloc, TlsAlloc, SwitchToThread, InitializeCriticalSectionAndSpinCount, SetLastError, DecodePointer, EncodePointer, MultiByteToWideChar, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, WideCharToMultiByte, FormatMessageW, GetLastError, GetConsoleWindow, CopyFileA, lstrcatW, WinExec, lstrcpyW, FindResourceW, SizeofResource, LockResource, LoadResource, GetModuleFileNameW, GetModuleFileNameA, VirtualAlloc, SetPriorityClass, SetThreadPriority, GetCurrentThread, GetCurrentProcess, GetShortPathNameW, GetEnvironmentVariableW, ExitThread, FreeLibraryAndExitThread, GetFileAttributesExW, PeekNamedPipe, SystemTimeToTzSpecificLocalTime, FileTimeToSystemTime, ReadConsoleA, DeleteFileW, RtlPcToFileHeader, RaiseException, RtlUnwindEx, LoadLibraryExW, ExitProcess, SetConsoleCtrlHandler, HeapFree
bcrypt.dll	BCryptGenRandom
WS2_32.dll	WSAIoctl, htons, getpeername, select, __WSAFDIsSet, WSAWaitForMultipleEvents, WSAResetEvent, WSAEnumNetworkEvents, WSACreateEvent, WSACloseEvent, socket, setsockopt, listen, connect, inet_pton, bind, WSAEventSelect, WSASetLastError, send, recv, freeaddrinfo, getaddrinfo, WSAGetLastError, WSACleanup, WSAStartup, ntohs, getsockopt, getsockname, ioctlsocket, ntohl, htonl, recvfrom, sendto, gethostname, closesocket, accept
CRYPT32.dll	CertFreeCertificateChain, CertGetCertificateChain, CertFreeCertificateChainEngine, CertCreateCertificateChainEngine, CryptQueryObject, CertGetNameStringA, CertFindExtension, CertAddCertificateContextToStore, CryptDecodeObjectEx, PFXImportCertStore, CryptStringToBinaryA, CertGetCertificateContextProperty, CertFreeCertificateContext, CertDuplicateCertificateContext, CertFindCertificateInStore, CertEnumCertificatesInStore, CertCloseStore, CertOpenStore
ADVAPI32.dll	CryptEncrypt, CryptImportKey, CryptHashData, CryptGenRandom, CryptGetHashParam, CryptAcquireContextA, CryptEnumProvidersW, CryptSignHashW, CryptDestroyHash, CryptCreateHash, CryptDecrypt, CryptExportKey, CryptGetUserKey, CryptGetProvParam, CryptSetHashParam, CryptDestroyKey, CryptReleaseContext, CryptAcquireContextW, ReportEventW, RegisterEventSourceW, DeregisterEventSource

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 18

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2022 11:18:25.255116940 CEST	49753	80	192.168.2.6	115.231.97.60
May 24, 2022 11:18:28.353368998 CEST	49753	80	192.168.2.6	115.231.97.60
May 24, 2022 11:18:34.356031895 CEST	49753	80	192.168.2.6	115.231.97.60
May 24, 2022 11:18:46.356165886 CEST	49774	80	192.168.2.6	180.101.136.19
May 24, 2022 11:18:49.370821953 CEST	49774	80	192.168.2.6	180.101.136.19
May 24, 2022 11:18:55.371294975 CEST	49774	80	192.168.2.6	180.101.136.19
May 24, 2022 11:19:11.680466890 CEST	49789	80	192.168.2.6	180.101.136.19
May 24, 2022 11:19:14.716696024 CEST	49789	80	192.168.2.6	180.101.136.19
May 24, 2022 11:19:20.717226028 CEST	49789	80	192.168.2.6	180.101.136.19
May 24, 2022 11:19:32.720256090 CEST	49794	80	192.168.2.6	115.231.97.60
May 24, 2022 11:19:35.718535900 CEST	49794	80	192.168.2.6	115.231.97.60
May 24, 2022 11:19:41.718998909 CEST	49794	80	192.168.2.6	115.231.97.60
May 24, 2022 11:19:56.655518055 CEST	49828	443	192.168.2.6	49.233.94.119
May 24, 2022 11:19:56.655560970 CEST	443	49828	49.233.94.119	192.168.2.6
May 24, 2022 11:19:56.655685902 CEST	49828	443	192.168.2.6	49.233.94.119
May 24, 2022 11:19:56.828752995 CEST	49828	443	192.168.2.6	49.233.94.119
May 24, 2022 11:19:56.828783035 CEST	443	49828	49.233.94.119	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2022 11:18:25.229048014 CEST	56591	53	192.168.2.6	8.8.8.8
May 24, 2022 11:18:25.248784065 CEST	53	56591	8.8.8.8	192.168.2.6
May 24, 2022 11:19:11.638067007 CEST	51194	53	192.168.2.6	8.8.8.8
May 24, 2022 11:19:11.659339905 CEST	53	51194	8.8.8.8	192.168.2.6
May 24, 2022 11:19:55.040888071 CEST	55083	53	192.168.2.6	8.8.8.8
May 24, 2022 11:19:55.348397970 CEST	53	55083	8.8.8.8	192.168.2.6

DNS Queries

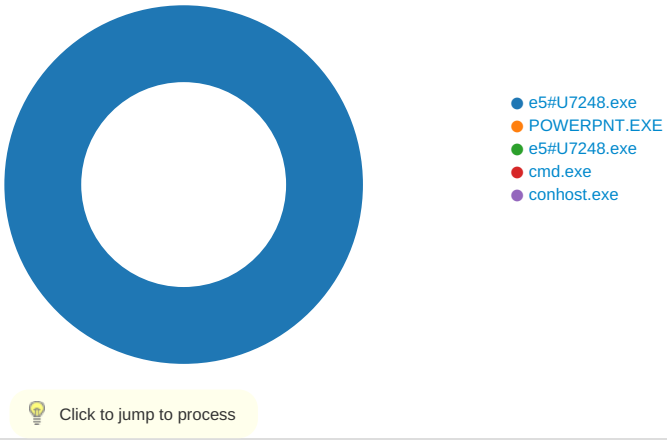
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 24, 2022 11:18:25.229048014 CEST	192.168.2.6	8.8.8.8	0xa156	Standard query (0)	rs.qbox.me	A (IP address)	IN (0x0001)
May 24, 2022 11:19:11.638067007 CEST	192.168.2.6	8.8.8.8	0xe907	Standard query (0)	rs.qbox.me	A (IP address)	IN (0x0001)
May 24, 2022 11:19:55.040888071 CEST	192.168.2.6	8.8.8.8	0x9872	Standard query (0)	service-ep07djah-1306669097.bj.apigw.tencentcs.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 24, 2022 11:18:25.248784065 CEST	8.8.8.8	192.168.2.6	0xa156	No error (0)	rs.qbox.me	kodo-elb-z0.qbox.me		CNAME (Canonical name)	IN (0x0001)
May 24, 2022 11:18:25.248784065 CEST	8.8.8.8	192.168.2.6	0xa156	No error (0)	kodo-elb-z0.qbox.me		115.231.97.60	A (IP address)	IN (0x0001)
May 24, 2022 11:18:25.248784065 CEST	8.8.8.8	192.168.2.6	0xa156	No error (0)	kodo-elb-z0.qbox.me		180.101.136.19	A (IP address)	IN (0x0001)
May 24, 2022 11:19:11.659339905 CEST	8.8.8.8	192.168.2.6	0xe907	No error (0)	rs.qbox.me	kodo-elb-z0.qbox.me		CNAME (Canonical name)	IN (0x0001)
May 24, 2022 11:19:11.659339905 CEST	8.8.8.8	192.168.2.6	0xe907	No error (0)	kodo-elb-z0.qbox.me		180.101.136.19	A (IP address)	IN (0x0001)
May 24, 2022 11:19:11.659339905 CEST	8.8.8.8	192.168.2.6	0xe907	No error (0)	kodo-elb-z0.qbox.me		115.231.97.60	A (IP address)	IN (0x0001)
May 24, 2022 11:19:55.348397970 CEST	8.8.8.8	192.168.2.6	0x9872	No error (0)	service-ep07djah-1306669097.bj.apigw.tencentcs.com	1-1.bj.apigwtencent.com		CNAME (Canonical name)	IN (0x0001)
May 24, 2022 11:19:55.348397970 CEST	8.8.8.8	192.168.2.6	0x9872	No error (0)	1-1.bj.apigwtencent.com		49.233.94.119	A (IP address)	IN (0x0001)
May 24, 2022 11:19:55.348397970 CEST	8.8.8.8	192.168.2.6	0x9872	No error (0)	1-1.bj.apigwtencent.com		140.143.115.153	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: e5#U7248.exe PID: **7116**, Parent PID: **4244**

General

Target ID:	1
Start time:	11:18:23
Start date:	24/05/2022
Path:	C:\Users\user\Desktop\e5#U7248.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\e5#U7248.exe"
Imagebase:	0x7ff6c97a0000
File size:	4937216 bytes
MD5 hash:	032E7E721DFE5DBC95BB91A3BC2E935C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: POWERPNT.EXE PID: **3256**, Parent PID: **7116**

General

Target ID:	11
Start time:	11:19:09
Start date:	24/05/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE" "C:\Users\user\Desktop\e5#U7248.pptx" /ou ''
Imagebase:	0x1040000
File size:	1849008 bytes
MD5 hash:	68F52CD14C61DDC941769B55AE3F2EE9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

Analysis Process: e5#U7248.exe PID: **6884**, Parent PID: **7116**

General

Target ID:	12
Start time:	11:19:09
Start date:	24/05/2022
Path:	C:\Users\Public\Music\e5#U7248.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\Music\e5#U7248.exe

Imagebase:	0x7ff79e5b0000
File size:	4937216 bytes
MD5 hash:	032E7E721DFE5DBC95BB91A3BC2E935C
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: 0000000C.00000002.631477810.000001C8CA0EB000.00000004.00000020.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 0000000C.00000002.631477810.000001C8CA0EB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Cobaltbaltstrike_RAW_Payload_https_stager_x64, Description: Detects CobaltStrike payloads, Source: 0000000C.00000002.631567397.000001C8CA290000.00000040.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 0000000C.00000002.631567397.000001C8CA290000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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

Analysis Process: cmd.exe PID: **820**, Parent PID: **7116**

General

Target ID:	16
Start time:	11:19:41
Start date:	24/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c del C:\Users\user\Desktop\e5#U7248.exe > nul
Imagebase:	0x7ff6edbd0000
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

Analysis Process: conhost.exe PID: **6852**, Parent PID: **820**

General

Target ID:	19
Start time:	11:19:45
Start date:	24/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly