ID: 632996
Sample Name: 05#U7248.exe
Cookbook: default.jbs
Time: 11:16:11
Date: 24/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

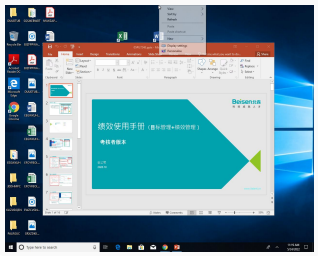
Windows Analysis Report

05#U7248.exe

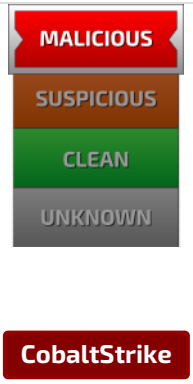
Overview

General Information

Sample Name:	05#U7248.exe
Analysis ID:	632996
MD5:	e178cc94333d53..
SHA1:	00b9b0cc846add..
SHA256:	2e536464425568.
Tags:	CobaltStrike exe
Infos:	



Detection



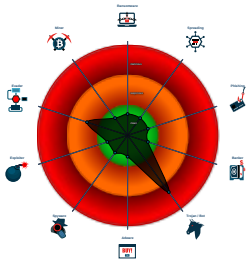
CobaltStrike

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- 05#U7248.exe (PID: 6452 cmdline: "C:\Users\user\Desktop\05#U7248.exe" MD5: E178CC94333D536AAF159B641AB71B2C)
  - POWERPNT.EXE (PID: 5676 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE" "C:\Users\user\Desktop\05#U7248.pptx" /ou " MD5: 68F52CD14C61DDC941769B55AE3F2EE9)
  - 05#U7248.exe (PID: 6716 cmdline: C:\Users\Public\Music\05#U7248.exe MD5: E178CC94333D536AAF159B641AB71B2C)
  - cmd.exe (PID: 768 cmdline: "C:\Windows\system32\cmd.exe" /c del C:\Users\user\Desktop\05#U7248.exe > nul MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6328 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
0000000F.00000002.520130307.000002BB3F020000.00000040.00001000.00020000.00000000.sdmp	Cobaltbaltstrike_RAW_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
0000000F.00000002.520130307.000002BB3F020000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_CobaltStrike_3	Yara detected CobaltStrike	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.519944929.000002BB3EE33000.00000004.00000020.00020000.00000000.sdmp	Cobaltbaltstrike_RAW_Payload_https_stager_x64	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0xa2e0:$h01: FC 48 83 E4 F0 E8 C8 00 00 00 41 51 41 50 52 51 56 48 31 D2 65 48 8B 52
0000000F.00000002.519944929.000002BB3EE33000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CobaltStrike_3	Yara detected CobaltStrike	Joe Security	
0000000F.00000003.517681669.000002BB3EE32000.00000004.00000020.00020000.00000000.sdmp	Cobaltbaltstrike_RAW_Payload_https_stager_x64	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0xb2e0:$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
Click to see the 1 entries				

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

Deletes itself after installation

Self deletion via cmd delete

Remote Access Functionality

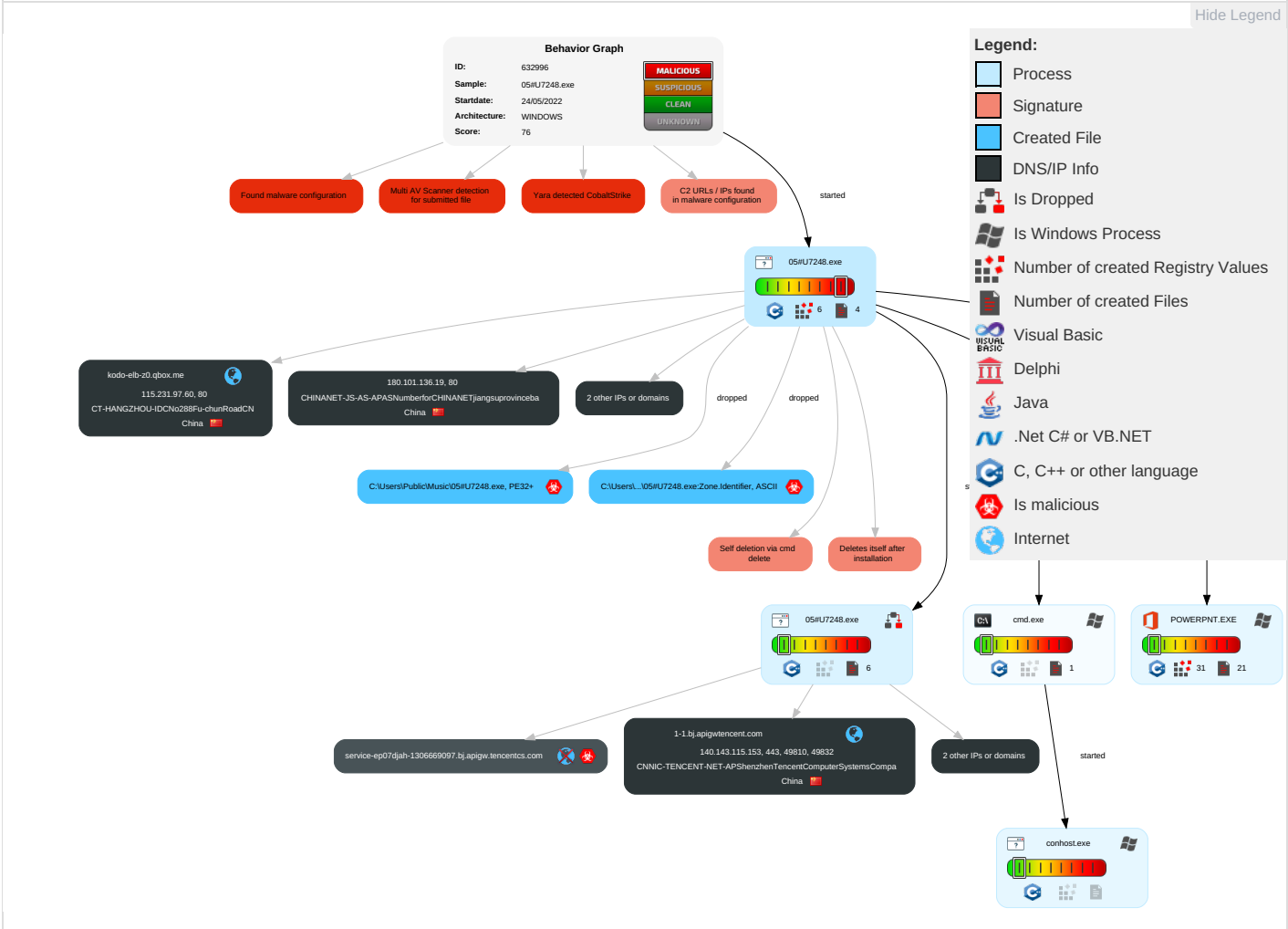
Yara detected CobaltStrike

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Process Injection	LSASS Memory	1 Security Software Discovery	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
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Extra Window Memory Injection	2 Obfuscated Files or Information	Security Account Manager	1 Remote System 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 File and Directory 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	3 System Information 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	System Owner/User 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

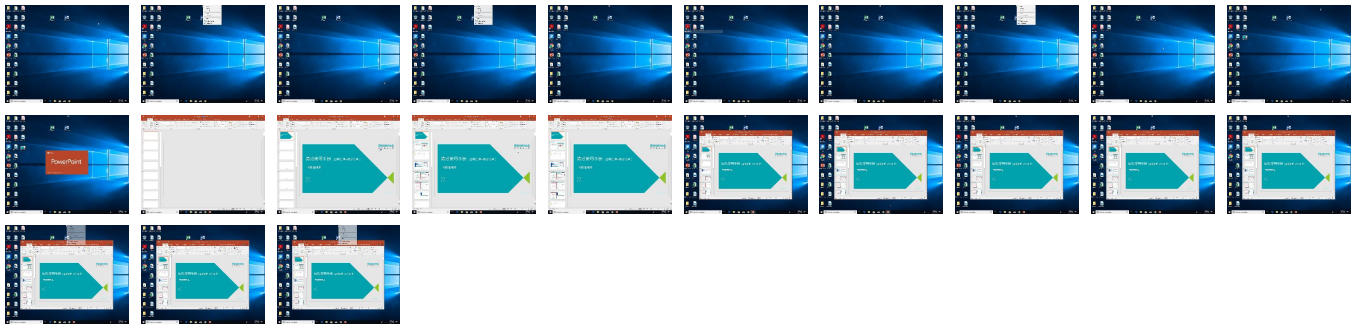
Behavior Graph

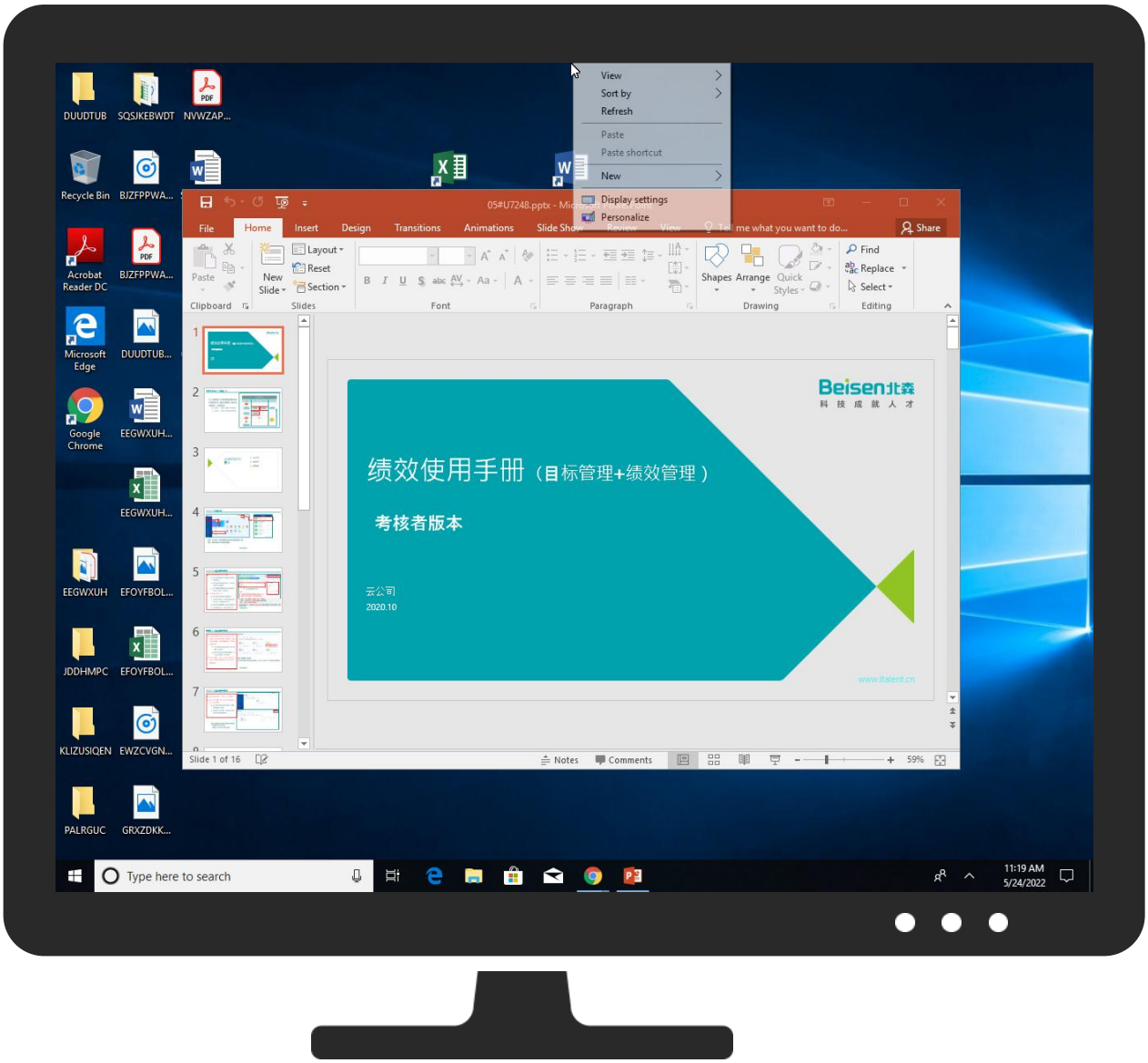


Screenshots

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
05#U7248.exe	9%	Virustotal		Browse
05#U7248.exe	3%	Metadefender		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Music\05#U7248.exe	3%	Metadefender		Browse

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%	Virustotal		Browse
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://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.js0	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://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://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.js.com	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.jsX	0%	Avira URL Cloud	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://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/xN	0%	Avira URL Cloud	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	140.143.115.153	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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

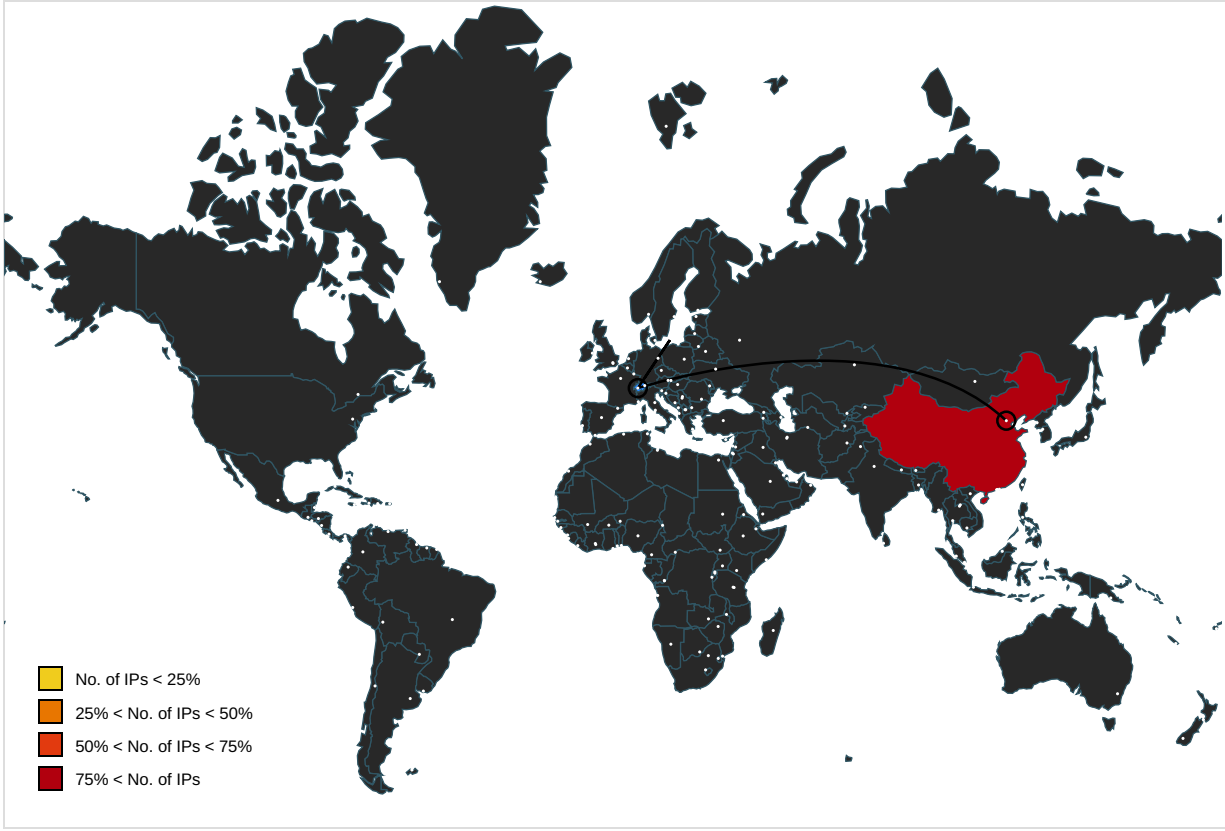
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://login.microsoftonline.com/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://shell.suite.office.com:1443	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://rs.qbox.me/chtype/RGJhay9jaGRiOnFpbml1LnBuZw==/type/1	05#U7248.exe, 0000000F.00000002.51988819 4.000002BB3EE08000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://autodiscover-s.outlook.com/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://roaming.edog.	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://cdn.entity.	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://powerlift.acompli.net	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://api.qiniu.com	05#U7248.exe, 05#U7248.exe.0.dr	false		high
http://https://cortana.ai	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://rs.qbox.mehttp://rsf.qbox.mehttp://api.qiniu.comhttp://fusion.qiniuapi.comhttp://uc.qbox.meht	05#U7248.exe, 05#U7248.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.onenote.com/upload.aspx	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://api.aadrm.com/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://rs.qbox.me/chtype/RGJhay9jaGRiOnFpbml1LnBuZw==/type/1da	05#U7248.exe, 0000000F.00000002.51988819 4.000002BB3EE08000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://curl.se/docs/hsts.html	05#U7248.exe, 05#U7248.exe.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.js	05#U7248.exe, 0000000F.00000002.52001014 8.000002BB3EE76000.00000004.00000020.000 20000.00000000.sdmp, 05#U7248.exe, 00000 00F.00000002.519888194.000002BB3EE08000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.js0	05#U7248.exe, 0000000F.00000002.51988819 4.000002BB3EE08000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://api.microsoftstream.com/api/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://cr.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://graph.ppe.windows.net	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://officeci.azurewebsites.net/api/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://upload.qiniup.com	05#U7248.exe, 05#U7248.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://rs.qbox.me/chtype/RGJhay9jaGRiOnFpbml1LnBuZw==/type/1_PM	05#U7248.exe, 00000000.00000002.42034141 9.000001A6926D8000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://store.office.cn/addinstemplate	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://globaldisco.crm.dynamics.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://messaging.engagement.office.com/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://dev0-api.acompli.net/autodetect	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://web.microsoftstream.com/video/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://curl.se/docs/alt-svc.html	05#U7248.exe, 05#U7248.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.js.com	05#U7248.exe, 0000000F.00000002.52001014 8.000002BB3EE76000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://graph.windows.net	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://dataservice.o365filtering.com/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/bootstrap-2.min.jsX	05#U7248.exe, 0000000F.00000003.51772769 9.000002BB3EE76000.00000004.00000020.000 20000.00000000.sdmp, 05#U7248.exe, 00000 00F.00000002.520010148.000002BB3EE76000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://analysis.windows.net/powerbi/api	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://ncus.contentsync.	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://weather.service.msn.com/data.aspx	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://apis.live.net/v5.0/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://management.azure.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://outlook.office365.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://wus2.contentsync.	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://iovip.qbox.me	05#U7248.exe, 05#U7248.exe.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://api.office.net	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://incidents.diagnosticssdf.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://fusion.qiniuapi.com	05#U7248.exe, 05#U7248.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://asgsmsproxyapi.azurewebsites.net/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://entitlement.diagnostics.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://service-ep07djah-1306669097.bj.apigw.tencentcs.com/xN	05#U7248.exe, 0000000F.00000002.52003153 8.000002BB3EE88000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://substrate.office.com/search/api/v2/init	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://outlook.office.com/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://outlook.office365.com/	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://webshell.suite.office.com	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	40C9AF57-D49E-46F0-BAA8-A9E834DB8605.14.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
180.101.136.19	unknown	China		23650	CHINANET-JS-AS-APASNumberforCHINANETjiangsuprovinceba	false
140.143.115.153	1-1.bj.apigwtencent.com	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632996
Start date and time: 24/05/202211:16:11	2022-05-24 11:16:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	05#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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.109.32.63, 52.109.88.38, 52.109.12.22
- Excluded domains from analysis (whitelisted): fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, 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 05#U7248.exe, PID 6452 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 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\05#U7248.exe

Process:	C:\Users\user\Desktop\05#U7248.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4654592
Entropy (8bit):	7.272750905471198
Encrypted:	false
SSDEEP:	98304:S0+E9G0Iv7XF4UNLQPrGR4C3hrx+LWGXHt9lOYN:fX9G0Iv714QX2C37+LWG3tH
MD5:	E178CC94333D536AAF159B641AB71B2C
SHA1:	00B9B0CC846ADD4164DDE07A4B03E357118A3126
SHA-256:	2E5364644255681AE085C113B6D88E4D3BC1DB18D3EF8C06B8264194A39687E9
SHA-512:	5268C9F1384D2A83DCF907FAC6D403603A560C54F3E4221325AD9BAC0345735EEE247DE8B6346949A30A68FE68FADF373FAC078111EC5E2A03D7CCD3529C9D6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....~r..:.y.:.y.:.y._u}...y._uz.6.y._u|...y.:.y.&.y.....=.y.h{z.3.y..z}.J.y._ux.5.y.:.x...y.h{|...y.h{}...y..z|.;.y..z..;.y.:...;.y..z{.;.y.Rich:.y.....PE..d...g].b.....".....d....).....@.....G.....`.....Z'.....@).....(..$.....@G.@]....&.....&.....text...$c.....d..... ..`.rdata.....h.....@..@.data.....'..2...Z'.....@....pdata...$....(..&....'.....@..@.rsrc.....@).....(.....@..@.reloc..@]...@G..^....F.....@..B.....

C:\Users\Public\Music\05#U7248.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\05#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\40C9AF57-D49E-46F0-BAA8-A9E834DB8605

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):	5.359234653552132
Encrypted:	false
SSDEEP:	1536:0cQk/gxgB5B3guw//Q9DQW+zQWk4F77nXmvidQXxFETLKz6e:GHQ9DQW+zIXQI
MD5:	6DCE90D2231A227E1B1E3C7E985C7626
SHA1:	5D1AC27CF1431B6E7C1C45EFDF19A2B5C8BD5B66
SHA-256:	08ABECD5EF0D04A7E40BE7E566AB1FA2B890BBA495BF0AC61B0BAB7BFA620960
SHA-512:	B654C8234C7B4B8E2AE68467105FA4C87928F0CCD0F9A8D4F1DB0B7AFF13B8B949E6DDF59E3BF34C91CFF71C90D5E2B0BA9A08E4B154509DFC68F2D18B536D2
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="2022-05-24T09:18:04">.. 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\05.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 17:18:00 2022, mtime=Tue May 24 17:18:03 2022, atime=Tue May 24 17:18:00 2022, length=1786211, window=hide
Category:	dropped
Size (bytes):	1050
Entropy (8bit):	4.706921663969832
Encrypted:	false
SSDEEP:	12:8APsA0UguElPCH2JpHwYVwEX+W+fJ1OtYjAj/IN6OND5IB5IT4t2Y+xIBjKZm:82ap2ECi8AjkDso7aB6m
MD5:	C2D6F5FD83AB0D52B21F90F2AB38BAB3
SHA1:	93D50891D8ED3B2DDA08E9B6AC37E6E1D28FD70D
SHA-256:	447F08D641F281E83B684F6F3E91D8DFFFC2AD7B58511F5F87D01846091AE18D
SHA-512:	A57265C63CE113508CCBF012F4BB489C62E05A952CA0FA0C52BEF7B7311AA23B3E9D1EF66C75C8C966A4729488DDE88DF6FE839B150092BB46F40AB7EF668ADF
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...6...o...>...o...|...o..cA.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...T(.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..T(.....S.....U(>.h.a.r.d.z.....~.1.....TA...Desktop.h.....Ny..TA.....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.cA...TA. .05#U72~1.PPT..L.....TA..TA.....Wl..0.5.#.U.7.2.4.8...p.p.t.x.....S.....-.....R.....>.S.....C:\Users\user\Desktop\05#U7248.pptx..$....\....\....\....\....\.D.e.s.k.t.o.p.\.0.5.#.U.7.2.4.8...p.p.t.x.....:..,.LB.)...As...`.....X.....971342.....!a..%.H.VZAj.....-..!a..%.H.VZAj.....-.....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...1SPS..mD..p

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):	56
Entropy (8bit):	4.412477530299485
Encrypted:	false
SSDEEP:	3:bDuMJlU2mxWPYv:bC9oC
MD5:	98C86299F2C435F64179C8C0E757B04E
SHA1:	04C4DC312287C5040F0FD3F2617E2AF395F40E4B
SHA-256:	CAC3EF4ED62A29C75BC11A282F4688978A809B4DC3CCC763B9697E3E5BFBAFA7
SHA-512:	623C42320A36384B61DA136D0D8FCAEDBF8EB6819999AD7563BFEF6C846A96D173377CC2325695DB1FA5BB85FB5D77225C29DEF198E61DBF7F55751A5134476A
Malicious:	false
Preview:	[folders]..Templates.LNK=0..05.LNK=0..[misc]..05.LNK=0..

C:\Users\user\Desktop\05#U7248.pptx	
Process:	C:\Users\user\Desktop\05#U7248.exe
File Type:	Microsoft PowerPoint 2007+
Category:	modified
Size (bytes):	1786211
Entropy (8bit):	7.820259682121925
Encrypted:	false
SSDEEP:	49152:wygP1ekWVeGR4CoyhPjDF+1R1/wnDi9hfE4NtewK+OYN5:6rGR4C3hrx+LWGXHt9lOYN5
MD5:	A2C1B9BA8FCE029F60A0AE9088FC375D
SHA1:	D5401E86CFCBD66F46EB2B1003225B7C2CBAC69F
SHA-256:	C902737C9A19E9317288751484945AFE958A0D01A451C7B69C55C42338E6D204
SHA-512:	3C2B9A66426CDE59E8D531ED33A9E75DFA41B5E83B296CEF7062D6B54110AA060B0814E5272ECE3071663E70D80B5205E61CF7BC4CD72A080F51D9936426E286
Malicious:	false
Preview:	PK.....!..L}.@.....[Content_Types].xml ...(.....o. ...'...x.b.n.)N...i?*....}I.0 Y...l'.S9u:..K.3w.. .q8..J$+0.+.,...d.J..9.q.itE..,.P.r..K..g.&.k.6.his.pN.....M...#3e*..4s.Y..^...P.t#Wk....fl)\.....$Z.Ir...r.:.~N{#~i..i..c...$.i-x.....,..e..G....]pm..aO.zd..M.7|.....1.....j.....y..T5...JU,+.l.b..1.q...>.+...f.....}..&..K.....N.&:.....E'..N.>:A6....*f..b...f..c..2fqJ.T..u..G....!....j.T;..v...;....r6.C.+....<...8..@...2.....n-...H..Y?.5

Static File Info

General

File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	7.272750905471198
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:	05#U7248.exe
File size:	4654592
MD5:	e178cc94333d536aaf159b641ab71b2c
SHA1:	00b9b0cc846add4164dde07a4b03e357118a3126
SHA256:	2e5364644255681ae085c113b6d88e4d3bc1db18d3ef8c06b8264194a39687e9
SHA512:	5268c9f1384d2a83dcf907fac6d403603a560c54f3e4221325ad9bac0345735eee247de8b6346949a30a68fe68fadf373fac078111ec5e2a03d7ccd3529c9d56
SSDEEP:	98304:S0+E9G0Iv7XF4UNLQPrGR4C3hrx+LWGXHt9lOYN:fX9G0Iv714QX2C37+LWG3tH
TLSH:	C526CF1AAB6508E4DCB6C2348A565633E7B1BC1527716BEB03A0F6771F33AD11E3A704
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:	0x628B5D67 [Mon May 23 10:09:43 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 00007F7CF49AB850h
dec eax
add esp, 28h
jmp 00007F7CF49AADDFh
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax

Instruction
mov ebx, ecx
jmp 00007F7CF49AAF71h
dec eax
mov ecx, ebx
call 00007F7CF4A9284Ah
test eax, eax
je 00007F7CF49AAF75h
dec eax
mov ecx, ebx
call 00007F7CF4A8557Ah
dec eax
test eax, eax
je 00007F7CF49AAF49h
dec eax
add esp, 20h
pop ebx
ret
dec eax
cmp ebx, FFFFFFFFh
je 00007F7CF49AAF68h
call 00007F7CF49ABC18h
int3
call 00007F7CF49ABC32h
int3
jmp 00007F7CF49ABC4Ch
int3
int3
int3
jmp 00007F7CF49AAF1Ch
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 00007F7CF49AAF72h
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
mov ecx, ecx
inc ecx

Instruction
test byte ptr [eax], 00000004h
dec esp
mov edx, ecx
je 00007F7CF49AAF75h
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 00007F7CF49AAF6Dh
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	0x1df5c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x281000	0x12498	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x474000	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	0.43268546249	data	5.72253868895	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	0x1df5c0	0x1df600	False	0.791137854465	data	7.67265893712	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x474000	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	0x1b4163	Microsoft PowerPoint 2007+	Chinese	China
FILE_DATA	0x4701e8	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	0x473398	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: 22

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

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2022 11:17:17.710534096 CEST	49727	80	192.168.2.3	115.231.97.60
May 24, 2022 11:17:20.756198883 CEST	49727	80	192.168.2.3	115.231.97.60
May 24, 2022 11:17:26.765521049 CEST	49727	80	192.168.2.3	115.231.97.60
May 24, 2022 11:17:38.865847111 CEST	49749	80	192.168.2.3	180.101.136.19
May 24, 2022 11:17:41.865118027 CEST	49749	80	192.168.2.3	180.101.136.19
May 24, 2022 11:17:47.865593910 CEST	49749	80	192.168.2.3	180.101.136.19
May 24, 2022 11:18:05.430113077 CEST	49761	80	192.168.2.3	180.101.136.19
May 24, 2022 11:18:08.601726055 CEST	49761	80	192.168.2.3	180.101.136.19
May 24, 2022 11:18:14.602289915 CEST	49761	80	192.168.2.3	180.101.136.19
May 24, 2022 11:18:26.949278116 CEST	49764	80	192.168.2.3	115.231.97.60
May 24, 2022 11:18:30.027067900 CEST	49764	80	192.168.2.3	115.231.97.60
May 24, 2022 11:18:36.025890112 CEST	49764	80	192.168.2.3	115.231.97.60
May 24, 2022 11:18:48.836710930 CEST	49810	443	192.168.2.3	140.143.115.153
May 24, 2022 11:18:48.836779118 CEST	443	49810	140.143.115.153	192.168.2.3
May 24, 2022 11:18:48.838099003 CEST	49810	443	192.168.2.3	140.143.115.153
May 24, 2022 11:18:48.884810925 CEST	49810	443	192.168.2.3	140.143.115.153
May 24, 2022 11:18:48.884875059 CEST	443	49810	140.143.115.153	192.168.2.3
May 24, 2022 11:19:21.129180908 CEST	49810	443	192.168.2.3	140.143.115.153
May 24, 2022 11:19:21.199660063 CEST	49832	443	192.168.2.3	140.143.115.153
May 24, 2022 11:19:21.199721098 CEST	443	49832	140.143.115.153	192.168.2.3
May 24, 2022 11:19:21.199862957 CEST	49832	443	192.168.2.3	140.143.115.153
May 24, 2022 11:19:21.200618982 CEST	49832	443	192.168.2.3	140.143.115.153
May 24, 2022 11:19:21.200647116 CEST	443	49832	140.143.115.153	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 24, 2022 11:17:17.650461912 CEST	57723	53	192.168.2.3	8.8.8.8
May 24, 2022 11:17:17.671446085 CEST	53	57723	8.8.8.8	192.168.2.3
May 24, 2022 11:18:05.400410891 CEST	65266	53	192.168.2.3	8.8.8.8
May 24, 2022 11:18:05.422116041 CEST	53	65266	8.8.8.8	192.168.2.3
May 24, 2022 11:18:48.499269009 CEST	60640	53	192.168.2.3	8.8.8.8
May 24, 2022 11:18:48.807219028 CEST	53	60640	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 24, 2022 11:17:17.650461912 CEST	192.168.2.3	8.8.8.8	0xa8d5	Standard query (0)	rs.qbox.me	A (IP address)	IN (0x0001)
May 24, 2022 11:18:05.400410891 CEST	192.168.2.3	8.8.8.8	0x5e3b	Standard query (0)	rs.qbox.me	A (IP address)	IN (0x0001)

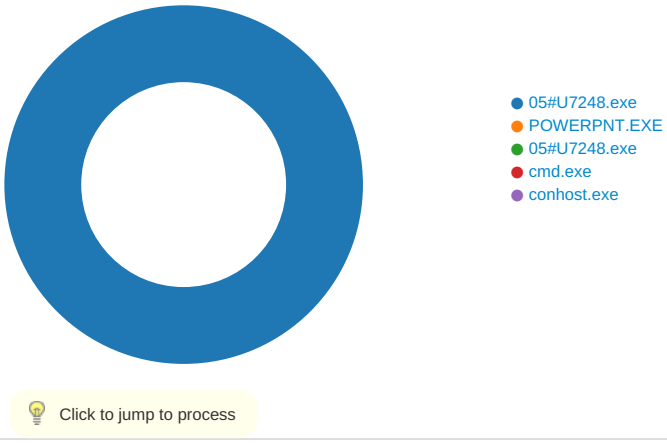
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 24, 2022 11:18:48.499269009 CEST	192.168.2.3	8.8.8.8	0xd76d	Standard query (0)	service-ep 07djah-130 6669097.bj .apigw.ten centcs.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 24, 2022 11:17:17.671446085 CEST	8.8.8.8	192.168.2.3	0xa8d5	No error (0)	rs.qbox.me	kodo-elb-z0.qbox.me		CNAME (Canonical name)	IN (0x0001)
May 24, 2022 11:17:17.671446085 CEST	8.8.8.8	192.168.2.3	0xa8d5	No error (0)	kodo-elb-z0.qbox.me		115.231.97.60	A (IP address)	IN (0x0001)
May 24, 2022 11:17:17.671446085 CEST	8.8.8.8	192.168.2.3	0xa8d5	No error (0)	kodo-elb-z0.qbox.me		180.101.136.19	A (IP address)	IN (0x0001)
May 24, 2022 11:18:05.422116041 CEST	8.8.8.8	192.168.2.3	0x5e3b	No error (0)	rs.qbox.me	kodo-elb-z0.qbox.me		CNAME (Canonical name)	IN (0x0001)
May 24, 2022 11:18:05.422116041 CEST	8.8.8.8	192.168.2.3	0x5e3b	No error (0)	kodo-elb-z0.qbox.me		180.101.136.19	A (IP address)	IN (0x0001)
May 24, 2022 11:18:05.422116041 CEST	8.8.8.8	192.168.2.3	0x5e3b	No error (0)	kodo-elb-z0.qbox.me		115.231.97.60	A (IP address)	IN (0x0001)
May 24, 2022 11:18:48.807219028 CEST	8.8.8.8	192.168.2.3	0xd76d	No error (0)	service-ep 07djah-130 6669097.bj .apigw.ten centcs.com	1-1.bj.apigwtencent.com		CNAME (Canonical name)	IN (0x0001)
May 24, 2022 11:18:48.807219028 CEST	8.8.8.8	192.168.2.3	0xd76d	No error (0)	1-1.bj.api gwtencent.com		140.143.115.153	A (IP address)	IN (0x0001)
May 24, 2022 11:18:48.807219028 CEST	8.8.8.8	192.168.2.3	0xd76d	No error (0)	1-1.bj.api gwtencent.com		49.233.94.119	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: 05#U7248.exe PID: **6452**, Parent PID: **5196**

General

Target ID:	0
Start time:	11:17:15
Start date:	24/05/2022

Path:	C:\Users\user\Desktop\05#U7248.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\05#U7248.exe"
Imagebase:	0x7ff7e23c0000
File size:	4654592 bytes
MD5 hash:	E178CC94333D536AAF159B641AB71B2C
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: 5676, Parent PID: 6452

General

Target ID:	14
Start time:	11:18:01
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\05#U7248.pptx" /ou "
Imagebase:	0xa0000
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: 05#U7248.exe PID: 6716, Parent PID: 6452

General	
Target ID:	15
Start time:	11:18:01
Start date:	24/05/2022
Path:	C:\Users\Public\Music\05#U7248.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\Music\05#U7248.exe
Imagebase:	0x7ff778370000
File size:	4654592 bytes
MD5 hash:	E178CC94333D536AAF159B641AB71B2C
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: 0000000F.00000002.520130307.000002BB3F020000.00000040.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 0000000F.00000002.520130307.000002BB3F020000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Cobaltbaltstrike_RAW_Payload_https_stager_x64, Description: Detects CobaltStrike payloads, Source: 0000000F.00000002.519944929.000002BB3EE33000.00000004.00000020.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 0000000F.00000002.519944929.000002BB3EE33000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Cobaltbaltstrike_RAW_Payload_https_stager_x64, Description: Detects CobaltStrike payloads, Source: 0000000F.00000003.517681669.000002BB3EE32000.00000004.00000020.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 0000000F.00000003.517681669.000002BB3EE32000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 3%, Metadefender, Browse
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: **768**, Parent PID: **6452**

General	
Target ID:	21
Start time:	11:18:34
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\05#U7248.exe > nul
Imagebase:	0x7ff63d570000
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: **6328**, Parent PID: **768**

General

Target ID:	22
Start time:	11:18:35
Start date:	24/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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