ID: 679126
Sample Name: 1a#U77e5.exe
Cookbook: default.jbs
Time: 09:54:36
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

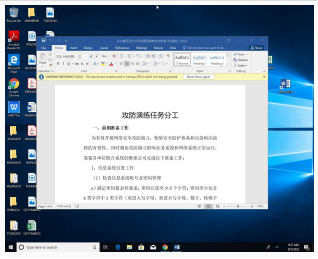
Windows Analysis Report

1a#U77e5.exe

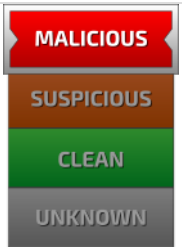
Overview

General Information

Sample Name:	1a#U77e5.exe
Analysis ID:	679126
MD5:	3f2202e24ad0a6..
SHA1:	62df51eb135127..
SHA256:	eb94cd39cde6a5..
Tags:	exe
Infos:	



Detection



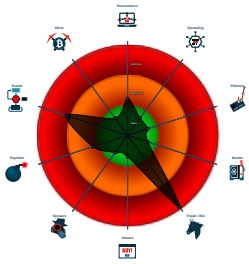
CobaltStrike

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected CobaltStrike
- C2 URLs / IPs found in malware con…
- Potentially malicious time measurem…
- Yara signature match
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- 1a#U77e5.exe (PID: 5296 cmdline: "C:\Users\user\Desktop\1a#U77e5.exe" MD5: 3F2202E24AD0A66C08F88A18DD7B5FB4)
  - ????????????.exe (PID: 3016 cmdline: C:\Windows\Temp\????????????.exe 9gb3vbgeng MD5: 84E3D79DA5E503374E61A17351781C14)
    - conhost.exe (PID: 5860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5788 cmdline: cmd.exe /c start ??????????????????????.docx MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 2164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - WINWORD.EXE (PID: 5308 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n "C:\U sers\user\Desktop\??????????????????????.docx" /o " MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

Threatname: CobaltStrike

```
{
  "BeaconType": [
    "HTTPS"
  ],
  "Port": 1443,
  "SleepTime": 60000,
  "MaxGetSize": 1048576,
  "Jitter": 0,
  "C2Server": "124.221.206.154,/submit.php",
  "HttpPostUri": "/submit.jsp",
  "Malleable_C2_Instructions": [],
  "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
  "HttpGet_Verb": "GET",
  "HttpPost_Verb": "POST",
  "HttpPostChunk": 0,
  "Spawnto_x86": "%windir%\\syswow64\\rundll32.exe",
  "Spawnto_x64": "%windir%\\sysnative\\rundll32.exe",
  "CryptoScheme": 0,
  "Proxy_Behavior": "Use IE settings",
  "Watermark": 0,
  "bStageCleanup": "False",
  "bCFGCaution": "False",
  "KillDate": 0,
  "bProcInject_StartRWX": "True",
  "bProcInject_UseRWX": "True",
  "bProcInject_MinAllocSize": 0,
  "ProcInject_PrependAppend_x86": "Empty",
  "ProcInject_PrependAppend_x64": "Empty",
  "ProcInject_Execute": [
    "CreateThread",
    "SetThreadContext",
    "CreateRemoteThread",
    "RtlCreateUserThread"
  ],
  "ProcInject_AllocationMethod": "VirtualAllocEx",
  "bUsesCookies": "True",
  "HostHeader": ""
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.706923007.000000C0002D6000.00000004.00001000.00020000.00000000.sdmp	Cobaltbaltstrike_Beacon_Encoded	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x0:$s10: TVpBUlVlieVIgewgAAAAS
00000003.00000002.705984762.000000C000174000.00000004.00001000.00020000.00000000.sdmp	Cobaltbaltstrike_Beacon_Encoded	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x10:$s10: TVpBUlVlieVIgewgAAAAS
00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp	HKTL_Meterpreter_inMemory	Detects Meterpreter in-memory	netbiosX, Florian Roth	• 0x3b3ae:$xs1: WS2_32.dll • 0x3b8a1:$xs2: ReflectiveLoader
00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp	Trojan_Raw_Generic_4	unknown	FireEye	• 0x17b4b:$s0: 83 C0 02 48 8B 7C 24 20 48 8B F0 B9 40 0 0 00 00 F3 A4 44 0F B6 84 24 A0 00 00 00 BA 40 00 00 0 0 48 8B 4C 24 20 E8 0F F3 FF FF 48 8B 54 24 20 48 8B 8C 24 98 00 00 00 48 8B 84 24 80 00 00 00 FF ... • 0x16f0e:$s1: 0F B7 00 3D 4D 5A 00 00 75 45 48 8B 44 2 4 20 48 63 40 3C 48 89 44 24 28 48 83 7C 24 28 40 72 2 F 48 81 7C 24 28 00 04 00 00 73 24 48 8B 44 24 20 48 8 B 4C 24 28 48 03 C8 48 8B C1 48 89 44 24 28 ...
00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp	CobaltStrike_Sleep_Decoder_Indicator	Detects CobaltStrike sleep_mask decoder	yara@s3c.za.net	• 0x10a48:$sleep_decoder: 48 89 5C 24 08 48 89 6C 24 1 0 48 89 74 24 18 57 48 83 EC 20 4C 8B 51 08 41 8B F0 48 8B EA 48 8B D9 45 8B 0A 45 8B 5A 04 4D 8D 52 08 4 5 85 C9
Click to see the 48 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.????????????.exe.25bf8a60000.2.raw.unpack	HKTL_Meterpreter_inMemory	Detects Meterpreter in-memory	netbiosX, Florian Roth	• 0x3a3ae:$xs1: WS2_32.dll • 0x3a8a1:$xs2: ReflectiveLoader

Source	Rule	Description	Author	Strings
3.2.????????????.exe.25bf8a60000.2.raw.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0x3a8a1:$x1: ReflectiveLoader
3.2.????????????.exe.25bf8a60000.2.raw.unpack	Cobaltbaltstrike_Beacon_x64	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x0:$h01: 4D 5A 41 52 55 48 89 E5 48 81 EC 20 00 00 00 48 8D 1D EA FF FF FF 48 89 • 0x3aa30:$h13: 2E 2F 2E 2F 2E 2C 2E 26 2E 2C 2E 2F 2E 2C 2B 8D 2E
3.2.????????????.exe.25bf8a60000.2.raw.unpack	CobaltStrike_Sleep_Decoder_Indicator	Detects CobaltStrike sleep_mask decoder	yara@s3c.za.net	• 0xfe48:$sleep_decoder: 48 89 5C 24 08 48 89 6C 24 10 48 89 74 24 18 57 48 83 EC 20 4C 8B 51 08 41 8B F0 48 8B EA 48 8B D9 45 8B 0A 45 8B 5A 04 4D 8D 52 08 45 85 C9
3.2.????????????.exe.25bf8a60000.2.raw.unpack	CobaltStrike_C2_Encoded_XOR_Config_Indicator	Detects CobaltStrike C2 encoded profile configuration	yara@s3c.za.net	• 0x3aa30:$s046: 2E 2F 2E 2F 2E 2C 2E 26 2E 2C 2E 2F 2E 2C 2B 8D 2E 2D 2E 2C 2E 2A 2E 2E C4 4E 2E 2A 2E 2C 2E 2A 2E 3E 2E 2E 2E 2B 2E 2F 2E 2C 2E 2E
Click to see the 59 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Anti Debugging

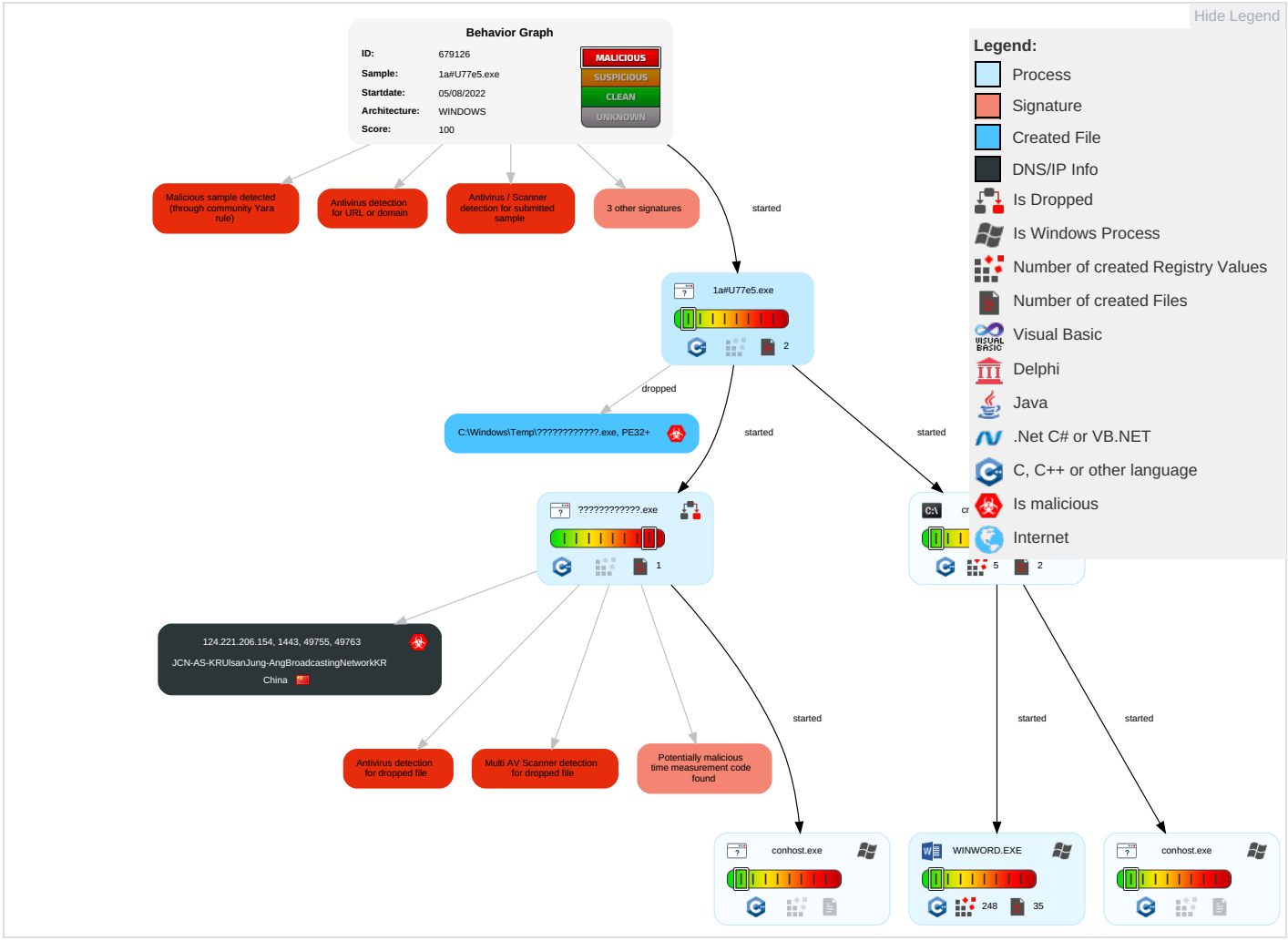
Potentially malicious time measurement code found

Remote Access Functionality

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	Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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 Deobfuscate/Decode Files or Information	NTDS	1 System Owner/User 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	3 Obfuscated Files or Information	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	1 Software Packing	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 DLL Side-Loading	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

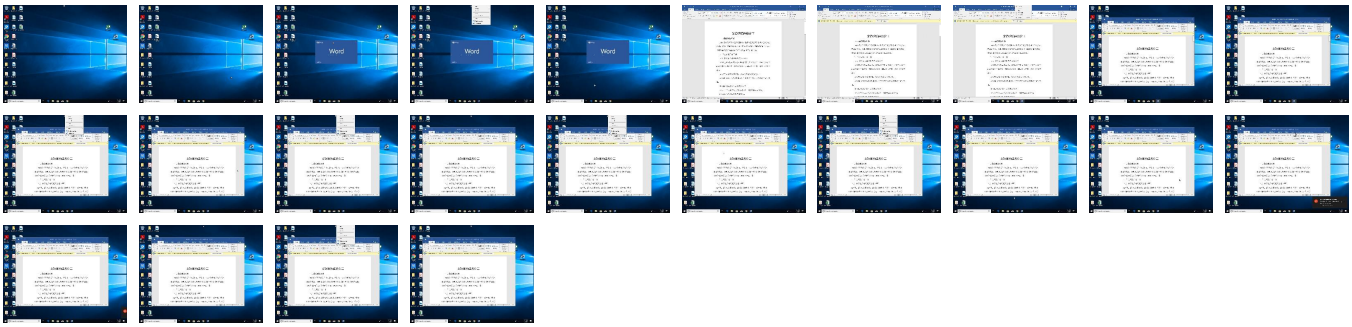
Behavior Graph

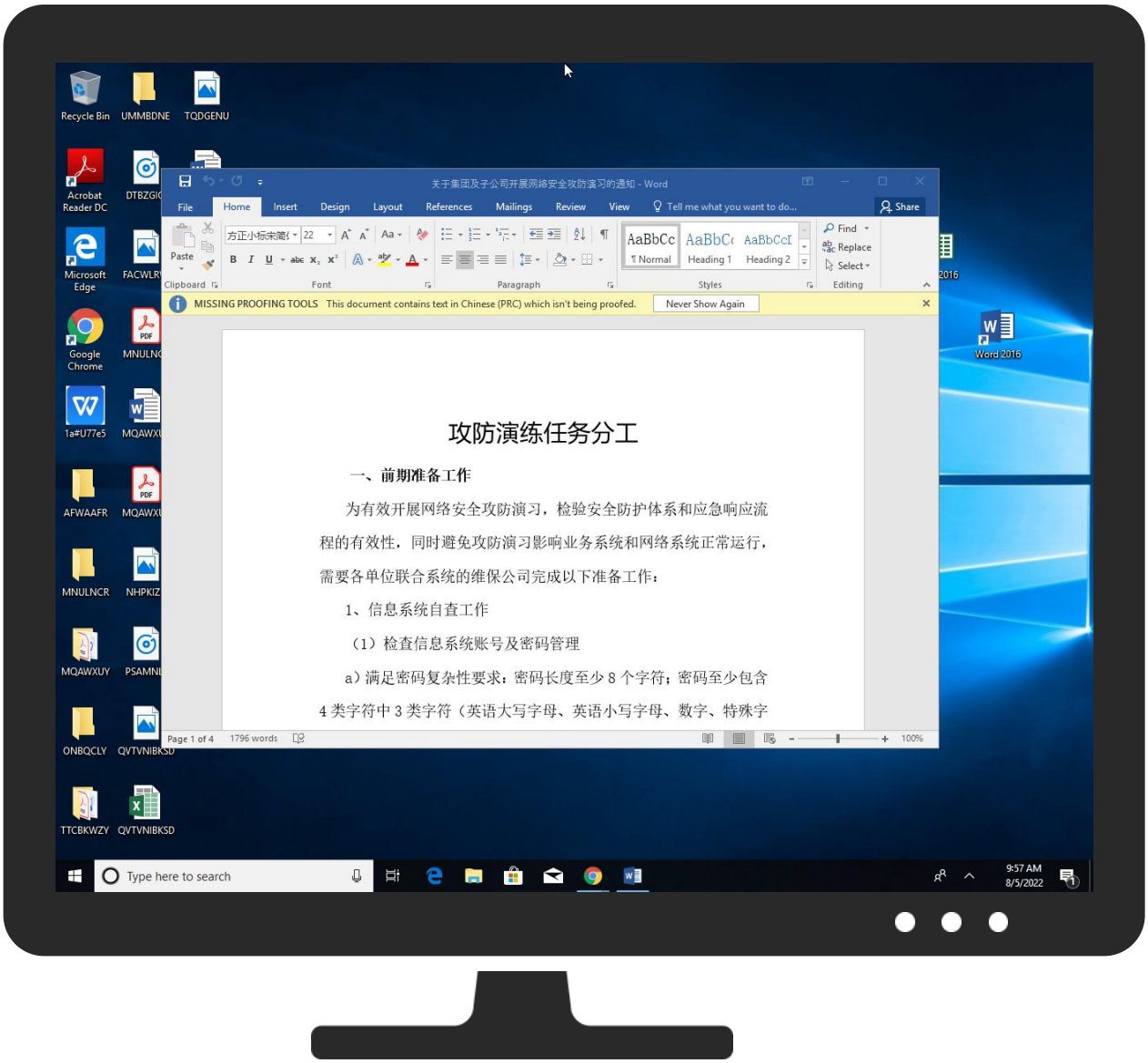


Screenshots

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
1a#U77e5.exe	61%	Virustotal		Browse
1a#U77e5.exe	23%	Metadefender		Browse
1a#U77e5.exe	77%	ReversingLabs	Win64.Trojan.CobaltStrike	
1a#U77e5.exe	100%	Avira	TR/CobaltStrike.fyzok	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\?????????????.exe	100%	Avira	HEUR/AGEN.1211767	
C:\Windows\Temp\?????????????.exe	26%	Metadefender		Browse
C:\Windows\Temp\?????????????.exe	62%	ReversingLabs	Win64.Downloader.Gobalt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.?????????????.exe.1300000.0.unpack	100%	Avira	HEUR/AGEN.1211767		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.1a#U77e5.exe.2a0000.0.unpack	100%	Avira	HEUR/AGEN.1211854		Download File
0.2.1a#U77e5.exe.2a0000.0.unpack	100%	Avira	HEUR/AGEN.1211854		Download File
3.0.????????????.exe.1300000.0.unpack	100%	Avira	HEUR/AGEN.1211767		Download File

Domains

No Antivirus matches

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://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://124.221.206.154:1443/ubmit.phpn	100%	Avira URL Cloud	malware	
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://124.221.206.154:1443/ubmit.php	100%	Avira URL Cloud	malware	
http://https://124.221.206.154/n-US	100%	Avira URL Cloud	malware	
http://https://my.microsoftpersonalcontent.com	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://124.221.206.154:1443/	100%	Avira URL Cloud	malware	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://124.221.206.154/W	100%	Avira URL Cloud	malware	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://124.221.206.154:1443/submit.phpo	100%	Avira URL Cloud	malware	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://124.221.206.154:1443/submit.phpw	100%	Avira URL Cloud	malware	
http://https://124.221.206.154:1443/submit.phpy	100%	Avira URL Cloud	malware	
http://https://124.221.206.154/-	100%	Avira URL Cloud	malware	
http://https://124.221.206.154:1443/submit.phpx	100%	Avira URL Cloud	malware	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
124.221.206.154	100%	Avira URL Cloud	malware	
http://https://124.221.206.154:1443/0;	100%	Avira URL Cloud	malware	
http://https://124.221.206.154:1443/submit.phpI	100%	Avira URL Cloud	malware	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://124.221.206.154:1443/submit.phpQ	100%	Avira URL Cloud	malware	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://124.221.206.154:1443/submit.phpc	100%	Avira URL Cloud	malware	
http://https://124.221.206.154:1443/submit.phpe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
124.221.206.154	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://login.microsoftonline.com/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://shell.suite.office.com:1443	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://autodiscover-s.outlook.com/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://roaming.edog.	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://cdn.entity.	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://powerlift.acompli.net	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://cortana.ai	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://api.aadrm.com/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://124.221.206.154:1443/ubmit.phpn	?????????????.exe, 00000003.00000002.7075 70619.0000025BF3699000.00000004.00000020 .00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://api.microsoftstream.com/api/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://cr.office.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://graph.ppe.windows.net	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tasks.office.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://officeci.azurewebsites.net/api/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://124.221.206.154:1443/ubmit.php	????????????.exe, 00000003.00000002.707570619.0000025BF3699000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://124.221.206.154/n-US	????????????.exe, 00000003.00000003.446429982.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.459728313.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.455168561.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.450683931.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.463998398.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://my.microsoftpersonalcontent.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://124.221.206.154:1443/	????????????.exe, 00000003.00000003.680436999.0000025BF36DA000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.528285189.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.511119713.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.450674237.0000025BF36D1000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.550870441.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.546326792.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.650269287.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.645708761.0000025BF36CD000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.546244712.0000025BF36CD000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.472618349.0000025BF36D1000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.446429982.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000002.707886816.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.459728313.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.515410872.0000025BF36D1000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.455168561.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.581376031.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000002.707824461.0000025BF36CD000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.555953821.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.507054004.0000025BF36D1000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.561061987.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.565779330.0000025BF36CD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://api.aadrm.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://globaldisco.crm.dynamics.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://messaging.engagement.office.com/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://dev0-api.acompli.net/autodetect	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://web.microsoftstream.com/video/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://dataservice.o365filtering.com/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://124.221.206.154/W	????????????.exe, 00000003.00000002.707682885.0000025BF36AC000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://officesetup.getmicrosoftkey.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://124.221.206.154:1443/submit.phpo	????????????.exe, 00000003.00000003.650269287.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000002.707886816.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.459728313.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.455168561.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.581376031.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.561061987.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.630445997.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.565837469.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.645791258.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.468267152.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.472644248.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.625692730.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.680612251.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.450683931.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.698330034.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.463998398.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.595821118.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://ncus.contentsync.	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://124.221.206.154:1443/submit.phpw	????????????.exe, 00000003.00000003.533004895.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://124.221.206.154:1443/submit.phpy	????????????.exe, 00000003.00000003.528285189.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.511119713.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.550870441.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.546326792.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.650269287.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000002.707886816.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.645791258.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.472644248.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.680612251.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.524018797.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.698330034.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.519760880.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.515437734.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.533004895.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.507141900.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://124.221.206.154/-	?????????????.exe, 00000003.00000003.528285189.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.511119713.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.550870441.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.546326792.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.446429982.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.459728313.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.455168561.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.581376031.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.555953821.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.561061987.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.565837469.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.468267152.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.472644248.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.450683931.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.524018797.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.519760880.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.515437734.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.463998398.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.533004895.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.507141900.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://124.221.206.154:1443/submit.phpx	?????????????.exe, 00000003.00000002.707682885.0000025BF36AC000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://weather.service.msn.com/data.aspx	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://apis.live.net/v5.0/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://124.221.206.154:1443/0;	?????????????.exe, 00000003.00000003.595821118.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://messaging.lifecycle.office.com/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://124.221.206.154:1443/submit.phpI	?????????????.exe, 00000003.00000003.528285189.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.550870441.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.546326792.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.555953821.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.561061987.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.680612251.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.524018797.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.698330034.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.519760880.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.515437734.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.533004895.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://management.azure.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://outlook.office365.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://wus2.contentsync.	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://124.221.206.154:1443/submit.phpQ	?????????????.exe, 00000003.00000003.511119713.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.446429982.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.459728313.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.455168561.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.565837469.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.468267152.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.472644248.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.450683931.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.463998398.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ?????????????.exe, 00000003.00000003.507141900.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://api.office.net	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://entitlement.diagnostics.office.com	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://substrate.office.com/search/api/v2/init	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://124.221.206.154:1443/submit.phpc	????????????.exe, 00000003.00000003.528285189.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.511119713.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.550870441.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.546326792.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.650269287.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000002.707886816.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.581376031.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.555953821.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.561061987.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.630445997.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.565837469.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.645791258.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.625692730.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.680612251.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.524018797.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.698330034.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.519760880.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.515437734.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.533004895.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.595821118.0000025BF36E3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://outlook.office.com/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://124.221.206.154:1443/submit.phpe	????????????.exe, 00000003.00000003.5282 85189.0000025BF36E3000.00000004.00000020 .00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.511119713.0000025BF 36E3000.00000004.00000020.00020000.00000 000.sdmp, ????????????.exe, 00000003.000 00003.550870441.0000025BF36E3000.0000000 4.00000020.00020000.00000000.sdmp, ????? ???????.exe, 00000003.00000003.546326792 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000003.650269287.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.446429982 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000002.707886816.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.459728313 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000003.455168561.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.581376031 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000003.555953821.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.561061987 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000003.630445997.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.565837469 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000003.645791258.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.468267152 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000003.472644248.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.625692730 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000003.680612251.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp, ????????????.exe, 00000003.00000003.450683931 .0000025BF36E3000.00000004.00000020.0002 0000.00000000.sdmp, ????????????.exe, 00 000003.00000003.524018797.0000025BF36E30 00.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://storage.live.com/clientlogs/uploadlocation	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high
http://https://outlook.office365.com/	E231148E-230F-4D9C-B6F4-7F66C34B8E20.7.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
124.221.206.154	unknown	China		45361	JCN-AS-KRUlsanJung-AngBroadcastingNetworkKR	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679126
Start date and time: 05/08/202209:54:36	2022-08-05 09:54:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1a#U77e5.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:	23
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:	mal100.troj.evad.winEXE@10/8@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 45.8% (good quality ratio 43%) • Quality average: 68.2% • Quality standard deviation: 27.6%

HCA Information:	• Successful, ratio: 81% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.88.191, 52.109.76.33, 52.109.12.21, 20.238.103.94, 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, asf-ris-prod-neu-azsc.northeurope.cloudapp.azure.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, licensing.mp.microsoft.com, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Execution Graph export aborted for target 1a#U77e5.exe, PID 5296 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:55:50	API Interceptor	30x Sleep call for process: ????????????.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E231148E-230F-4D9C-B6F4-7F66C34B8E20

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	148061

Entropy (8bit):	5.35816450806037
Encrypted:	false
SSDEEP:	1536:ncQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:W1Q9DQe+zuXYr
MD5:	DD89B24BAA865B152396CB932251EA2F
SHA1:	D0DB98C4FE2E281C64DF4F44DF5279F34E56DB54
SHA-256:	E25E7342FAD7C59D3D7E5F224BC370F1541CE3AD01FAF4C922F84F71137AF827
SHA-512:	E6599769C65FE10E4E70997B37F2A343BB6169C3FD09DB837A51386BE4E5DA019AF389D1AF09DABF60A80FD45F2347F6244930AA4AEBBE31066772D048039880
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-08-05T07:55:52">.. Build: 16.0.15601.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\??????????????????.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Fri Aug 5 15:55:47 2022, mtime=Fri Aug 5 15:55:52 2022, atime=Fri Aug 5 15:55:47 2022, length=16768, window=hide
Category:	dropped
Size (bytes):	1231
Entropy (8bit):	5.014235188340708
Encrypted:	false
SSDEEP:	12:81t6bU9G6CHihArh3GXqDkDlM8+WABe1OW7EO/ypaZFVW7LVW7KNDyffD4t2Y+x4:81ZArsUkDuPW7EOKqW7hW7ODyR7aB6m
MD5:	355E58BF021D90BF3CCDCD8503F910A1
SHA1:	34D3B542D1ABDD5B042B1BF790EEBD705899BFAC
SHA-256:	F40C4F240348D97AB8EB36F2DAA14F896B297339E8E2581A84AEC5AB20AB7AFD
SHA-512:	5A17937914179F6E98746DC8D45C82632DA16361A5E126E9403C74AC741E3D69FBF081B14FF1DDB7FDC4948C957ED0FDEBCB9C9B069D84069A21C6A4FB488AF
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...g.5...}-.8.../S.5....A.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...U.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....hT....user..>.....NM..U.....S.....`..a.l.f.o.n.s.....~.1.....U....Desktop.h.....NM..U.....Y.....>....."Y.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..A...U.. .6ADF~1.DOC..f.....U...U.....V.sQ.N..V.SP[lQ.S._U\Q..~.[hQ;e2..o`N.v...w..d.o.c.x.....$.....$...5.....h.....>.S.....C:\Users\user\Desktop\??????????????????????.docx.C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.D.e.s.k.t.o.p.\.sQ.N..V.SP[lQ.S._U\Q..~.[hQ;e2..o`N.v...w..d.o.c.x.....1.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.sQ.N..V.SP[lQ.S._U\Q..~.[hQ;e2..o`N.v...w..d.o.c.x.....:..,.LB.)...Aw..`.....X.....927537.....!a..%.H.VZAj.....s.....W...!a..%.H.VZAj..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	94
Entropy (8bit):	3.408464248242645
Encrypted:	false
SSDEEP:	3:bDuMJlWt6lmxWLRt6lv:bCNkRS
MD5:	113750065807DAD15C00A178EB21FC45
SHA1:	903505EE9B97E1FA7F39E9B9ECE4DE9B286E9289
SHA-256:	04AFC953D6AAE679A3ABDBE0FF0B8C144B16D4CCF84959A2793E57F6777AB8DF
SHA-512:	1F89B0584EEB6381314116748832AF82310053B659721AD6A07041FEAAA8E03E1A0EAF4C5400E1BBBB415B4A678C2C20F788AB8A69A6E2BB06436FB8B7C2DF8B
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..??????????????????????.LNK=0..[misc]..??????????????????????.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.9237687128468073
Encrypted:	false

SSDEEP:	3:Rl/Zdn98Udk1+lllllzHLl+l/Lcalt13l/9l:RtZT8Uq0ll/Ml/V
MD5:	8DCBD88C0E65C7ECD29DAE006EE77D62
SHA1:	EC6B2ADD4B3D90DB15700AC4D17BD605A33C870F
SHA-256:	B1895309312CB6286E97EE77C39BDF25D76C3298190EADB8DB26D487D2E3C7DF
SHA-512:	876FAF0B0681079CFA978F84C0BA46318998807C29811E4874D166F66D1E6E241E2237AEB26498E823193885E05BCDA230C357A91B640C35204D031333ECDC2A
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....L+....9i.0.....f.....q...5i.1.../.....1i.2.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..p.r.a.t.e.s.h.....

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

Process:	C:\Users\user\Desktop\1a#U77e5.exe
File Type:	Zip archive data, at least v1.0 to extract
Category:	dropped
Size (bytes):	16768
Entropy (8bit):	7.828953909266841
Encrypted:	false
SSDEEP:	384:aYn7elOjZppldfDmfFPpT83uzRz/4id7miP9jT:aYnKlOjZPldfDMFPG+zRz5p
MD5:	5F48BBB1AAC3B8D63AAAE3EC114BA340
SHA1:	31FC3508AF156D67DA4BC6FE8D41206BDA5276EE
SHA-256:	80596668ABC2C8C42481AD06713039198F08EB11C543061C3F9657A51248D04F
SHA-512:	F5C3AF4E2269094C5381C512AE2A13C8204A34477DD47DB5D7ED4FC7BC986ECB36B2EF17B0A7470D1CB64404B8035CB7D27563C45E7F8E94FA92CFB9E3F6B9E8
Malicious:	false
Preview:	PK.....N.@.....docProps/PK.....N.@...j...|.....docProps/app.xml.R.N.0..#..Q...-....'...@..r..Eb[.A..q^Q.Wn;3.x.c.....WF.R..4A-M..a.>7.."M|.....J....~y..g,...'.B.U.`...A.<.:*{..."t.b.{%.....u .....6.g...x...j..9../.....l/...c.>oM...Y..z>.r.`g\.y.,..F.;..qS.UU.dB....8..9M.....<.....o.|A.}?..R.X..|/z.@~..7.l.s7>.[.MN..T.V.1.,.Y'.....!V.w.m....W....r.f W.....W.uVT.:...6[...hY.s.....@.N...|w*.9.2.q....PK.....N.@N..e.....docProps/core.xml}..N.1...H.....$..Y$Z.T.J.*.....)*.K...@j..K.y..q.+..I.A .3..7.x...4..u*3]D...`D&..t.a ..vP.<7.....C{..V,r&2..l....\P..c"..9..!h.....j...p...>.....<..s\..&..R.....i...C...w.6(...`.{...l(...iew.-.X.O.....1nV6.....X..*S.....RT..=....u.S..~.%..hH....I..e.|..Z../.KVf...2....H.....Ir.....t1 ...].~}.]....._.?|.....ySm[.@...B..I.O[l.....k@RZ.0R..K..N5.NT...<.PK.....N.@....'.....docProps/custom.xml...K.0....C.=....mG. .....4..MR.t:.....}.{..E..(..

C:\Users\user\Desktop\~$??????????????????.docx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.9237687128468073
Encrypted:	false
SSDEEP:	3:Rl/Zdn98Udk1+lllllzHLl+l/Lcalt13l/9l:RtZT8Uq0ll/Ml/V
MD5:	8DCBD88C0E65C7ECD29DAE006EE77D62
SHA1:	EC6B2ADD4B3D90DB15700AC4D17BD605A33C870F
SHA-256:	B1895309312CB6286E97EE77C39BDF25D76C3298190EADB8DB26D487D2E3C7DF
SHA-512:	876FAF0B0681079CFA978F84C0BA46318998807C29811E4874D166F66D1E6E241E2237AEB26498E823193885E05BCDA230C357A91B640C35204D031333ECDC2A
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....L+....9i.0.....f.....q...5i.1.../.....1i.2.....

C:\Windows\Temp\???????????.exe

Process:	C:\Users\user\Desktop\1a#U77e5.exe
File Type:	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	2062848
Entropy (8bit):	6.989271790744726
Encrypted:	false
SSDEEP:	24576:VLG1BKsKoBqgde0DTIK2u4WXr3R0lgaWPPCwha1w0UHfLBamlNRDz:VLGKTZBermgaWPPCwha14/LR
MD5:	84E3D79DA5E503374E61A17351781C14
SHA1:	6C4710E5E6BC0F991C6954E64E76EC8BF796A2E1
SHA-256:	6254E9F7F9E61A1A80E8A3C01757B8D29C9AC0EB0D596236FC0A2944FD44DFD6
SHA-512:	B287D405B01AAA7B7C35AE1787395CCE626A4565B28BB74D2AA715D251D580AAB4EEE513D29885728B56F0175CB13238B6DCF0EC228DB83C6AC90CA7EEECC4D8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....*..9.....".....Z.....`.....@.....%..... ..`... .....#.|.....$..%..... Q..@.....text..... ..`.rdata...#... ...$.....@. .@.data.....P...Z...:.....@.../4.....'....P.....@..B/19....=x...`...z.....@..B/32.....I.....J.....@..B/46....*....0.....Z.....@..B/65.....-....@.... ...\.....@..B/78....I_....".`...*.....@..B/90.....|r...p#..t.....@..B.idata..|....#.....@....reloc...%....$..&.....@..B.symtab..O...0$..P...*..... .B.....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.725931255932212
TrID:	• Win64 Executable (generic) (12005/4) 74.95% • Generic Win/DOS Executable (2004/3) 12.51% • DOS Executable Generic (2002/1) 12.50% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	1a#U77e5.exe
File size:	4732928
MD5:	3f2202e24ad0a66c08f88a18dd7b5fb4
SHA1:	62df51eb1351279afa4dbe5920758d6974427ac9
SHA256:	eb94cd39cde6a5270181d6e6788c69a2a90ab2b27f9236c8382e810e4dfead1d
SHA512:	cd87c99ce09a29a5317343e04bb55fd63cd0b98cebcb08793a9b1dd275a9c6ce09c53fb7f901fc6083d8992360d3fbe02438d4143a907be64e7bdca15567bc27
SSDEEP:	49152:BuZC3FJrb/TWvO90dL3BmAFd4A64nsfJ+WNq3v3MVkOHx3bEnnkY3Xw4g9MUth7A:aC3F0uKUrwUZ0
TLSH:	2426BF333982B8FADAAD697184242D411D7CB88B172053C7BB4975FE36BA2D44D3C768
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....F.P.....".....~.....@.....@.....PN.....`... .....

File Icon

Icon Hash:	554d5c5469694525

Static PE Info

General

Entrypoint:	0x45ca40
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	

CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	9cbefe68f395e67356e2a5d8d1b285c0

Entrypoint Preview

Instruction
jmp 00007FAA8CC452C0h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
pushfd
cld
dec eax
sub esp, 000000E0h
dec eax
mov dword ptr [esp], edi
dec eax
mov dword ptr [esp+08h], esi
dec eax
mov dword ptr [esp+10h], ebp
dec eax
mov dword ptr [esp+18h], ebx
dec esp
mov dword ptr [esp+20h], esp
dec esp
mov dword ptr [esp+28h], ebp
dec esp
mov dword ptr [esp+30h], esi
dec esp
mov dword ptr [esp+38h], edi
movups dqword ptr [esp+40h], xmm6

Instruction
movups dqword ptr [esp+50h], xmm7
inc esp
movups dqword ptr [esp+60h], xmm0
inc esp
movups dqword ptr [esp+70h], xmm1
inc esp
movups dqword ptr [esp+00000080h], xmm2
inc esp
movups dqword ptr [esp+00000090h], xmm3
inc esp
movups dqword ptr [esp+000000A0h], xmm4
inc esp
movups dqword ptr [esp+000000B0h], xmm5
inc esp
movups dqword ptr [esp+000000C0h], xmm6
inc esp
movups dqword ptr [esp+000000D0h], xmm7
dec eax
sub esp, 30h
dec ecx
mov edi, eax
dec eax
mov edx, dword ptr [00000028h]
dec eax
cmp edx, 00000000h
jne 00007FAA8CC48F4Eh
dec eax
mov eax, 00000000h
jmp 00007FAA8CC48FC5h
dec eax
mov edx, dword ptr [edx+00000000h]
dec eax
cmp edx, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4c6000	0x47c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4e2000	0x2678	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4c7000	0x2b0a	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3cf140	0x140	.data
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	0x8fc6a	0x8fe00	False	0.4675638710903562	data	6.177951506515494	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x91000	0x33d8f0	0x33da00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3cf000	0x720a0	0x17e00	False	0.35497791230366493	data	4.298912004398371	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
/4	0x442000	0x127	0x200	False	0.6171875	data	5.097874074212899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/19	0x443000	0x1d578	0x1d600	False	0.9987782579787234	data	7.993303104291631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/32	0x461000	0x5b0b	0x5c00	False	0.9890455163043478	data	7.917262410977086	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/46	0x467000	0x2a	0x200	False	0.091796875	data	0.7534025800416837	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/65	0x468000	0x34e35	0x35000	False	0.9983048349056604	data	7.995735953621072	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/78	0x49d000	0x1e401	0x1e600	False	0.9892698688271605	data	7.987159878797264	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/90	0x4bc000	0x977c	0x9800	False	0.9757401315789473	data	7.788382558202588	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.idata	0x4c6000	0x47c	0x600	False	0.3313802083333333	data	3.514698326038637	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x4c7000	0x2b0a	0x2c00	False	0.3710049715909091	data	5.397043934669771	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.symtab	0x4ca000	0x17c10	0x17e00	False	0.2733045647905759	data	5.119810305846417	IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x4e2000	0x2678	0x2800	False	0.43115234375	data	5.682287008823302	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4e20b8	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4280181209, next used block 4280181211	English	United States
RT_GROUP_ICON	0x4e4660	0x14	data	English	United States

Imports

DLL	Import

DLL	Import
kernel32.dll	WriteFile, WriteConsoleW, WaitForMultipleObjects, WaitForSingleObject, VirtualQuery, VirtualFree, VirtualAlloc, SwitchToThread, SuspendThread, SetWaitableTimer, SetUnhandledExceptionFilter, SetProcessPriorityBoost, SetEvent, SetErrorMode, SetConsoleCtrlHandler, ResumeThread, PostQueuedCompletionStatus, LoadLibraryA, LoadLibraryW, SetThreadContext, GetThreadContext, GetSystemInfo, GetSystemDirectoryA, GetStdHandle, GetQueuedCompletionStatusEx, GetProcessAffinityMask, GetProcAddress, GetEnvironmentStringsW, GetConsoleMode, FreeEnvironmentStringsW, ExitProcess, DuplicateHandle, CreateWaitableTimerExW, CreateThread, CreateIoCompletionPort, CreateFileA, CreateEventA, CloseHandle, AddVectoredExceptionHandler

Possible Origin

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

Network Behavior

TCP Packets

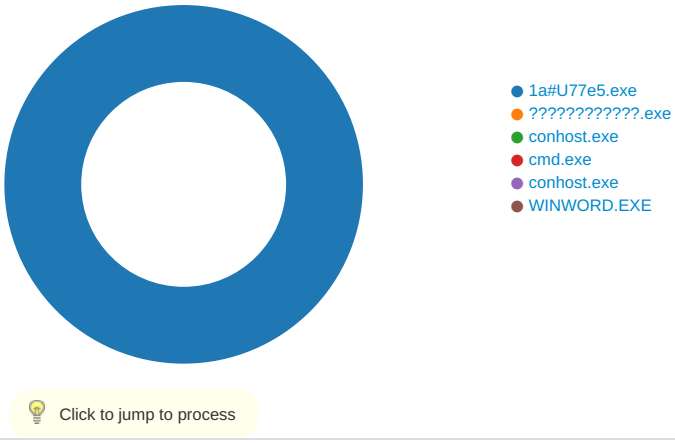
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:55:49.280426979 CEST	49755	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:49.470936060 CEST	1443	49755	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:50.056755066 CEST	49755	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:50.248254061 CEST	1443	49755	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:50.846036911 CEST	49755	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:51.035944939 CEST	1443	49755	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:51.151525021 CEST	49763	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:51.379904985 CEST	1443	49763	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:52.049324036 CEST	49763	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:52.277442932 CEST	1443	49763	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:52.846239090 CEST	49763	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:53.069526911 CEST	1443	49763	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:53.273742914 CEST	49767	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:53.499203920 CEST	1443	49767	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:54.049468994 CEST	49767	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:54.277996063 CEST	1443	49767	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:54.846920013 CEST	49767	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:55.072638988 CEST	1443	49767	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:55.255032063 CEST	49769	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:55.474117041 CEST	1443	49769	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:56.049721003 CEST	49769	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:56.268788099 CEST	1443	49769	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:56.846615076 CEST	49769	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:57.066648006 CEST	1443	49769	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:57.245265007 CEST	49776	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:57.465364933 CEST	1443	49776	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:58.065488100 CEST	49776	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:58.281260014 CEST	1443	49776	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:58.846745014 CEST	49776	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:59.065027952 CEST	1443	49776	124.221.206.154	192.168.2.5
Aug 5, 2022 09:55:59.198276997 CEST	49777	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:55:59.424679041 CEST	1443	49777	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:00.065619946 CEST	49777	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:00.291865110 CEST	1443	49777	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:00.862615108 CEST	49777	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:01.089356899 CEST	1443	49777	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:01.561662912 CEST	49778	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:01.754937887 CEST	1443	49778	124.221.206.154	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:56:02.363183022 CEST	49778	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:02.557374001 CEST	1443	49778	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:03.065870047 CEST	49778	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:03.259234905 CEST	1443	49778	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:03.430304050 CEST	49779	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:03.645586967 CEST	1443	49779	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:04.238054037 CEST	49779	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:04.453716993 CEST	1443	49779	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:05.050407887 CEST	49779	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:05.266046047 CEST	1443	49779	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:05.413183928 CEST	49780	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:05.616344929 CEST	1443	49780	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:06.238074064 CEST	49780	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:06.441137075 CEST	1443	49780	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:07.050636053 CEST	49780	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:07.253810883 CEST	1443	49780	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:07.442192078 CEST	49781	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:07.682126999 CEST	1443	49781	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:08.253863096 CEST	49781	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:08.493702888 CEST	1443	49781	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:09.066442966 CEST	49781	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:09.306078911 CEST	1443	49781	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:09.483295918 CEST	49782	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:12.566765070 CEST	49782	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:12.794334888 CEST	1443	49782	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:13.363702059 CEST	49782	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:25.599271059 CEST	49793	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:25.793513060 CEST	1443	49793	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:26.364763021 CEST	49793	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:26.559653997 CEST	1443	49793	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:27.067987919 CEST	49793	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:27.262059927 CEST	1443	49793	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:27.453006983 CEST	49805	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:27.669214964 CEST	1443	49805	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:28.239979029 CEST	49805	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:28.455928087 CEST	1443	49805	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:29.052509069 CEST	49805	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:29.268527985 CEST	1443	49805	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:29.495060921 CEST	49810	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:29.720386982 CEST	1443	49810	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:30.255779982 CEST	49810	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:30.481199026 CEST	1443	49810	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:31.068296909 CEST	49810	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:31.292104006 CEST	1443	49810	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:31.450253010 CEST	49816	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:31.668453932 CEST	1443	49816	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:32.255995035 CEST	49816	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:32.475545883 CEST	1443	49816	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:33.068542957 CEST	49816	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:33.286715031 CEST	1443	49816	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:33.424062014 CEST	49821	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:33.625540972 CEST	1443	49821	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:34.240472078 CEST	49821	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:34.441996098 CEST	1443	49821	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:35.053042889 CEST	49821	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:35.255081892 CEST	1443	49821	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:35.415158987 CEST	49829	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:35.633347034 CEST	1443	49829	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:36.240658045 CEST	49829	1443	192.168.2.5	124.221.206.154

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:56:36.458710909 CEST	1443	49829	124.221.206.154	192.168.2.5
Aug 5, 2022 09:56:37.053587914 CEST	49829	1443	192.168.2.5	124.221.206.154
Aug 5, 2022 09:56:37.271845102 CEST	1443	49829	124.221.206.154	192.168.2.5

Statistics

Behavior



System Behavior

Analysis Process: 1a#U77e5.exe PID: **5296**, Parent PID: **5884**

General

Target ID:	0
Start time:	09:55:44
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\1a#U77e5.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\1a#U77e5.exe"
Imagebase:	0x2a0000
File size:	4732928 bytes
MD5 hash:	3F2202E24AD0A66C08F88A18DD7B5FB4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: ????????????.exe PID: **3016**, Parent PID: **5296**

General

Target ID:	3
Start time:	09:55:46
Start date:	05/08/2022
Path:	C:\Windows\Temp\????????????.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Temp\????????????.exe 9gb3vbgeng

Imagebase:	0x1300000
File size:	2062848 bytes
MD5 hash:	84E3D79DA5E503374E61A17351781C14
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Cobaltbaltstrike_Beacon_Encoded, Description: Detects CobaltStrike payloads, Source: 00000003.00000002.706923007.000000C0002D6000.00000004.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: Cobaltbaltstrike_Beacon_Encoded, Description: Detects CobaltStrike payloads, Source: 00000003.00000002.705984762.000000C000174000.00000004.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: HKTL_Meterpreter_inMemory, Description: Detects Meterpreter in-memory, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: netbiosX, Florian Roth • Rule: Trojan_Raw_Generic_4, Description: unknown, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: FireEye • Rule: CobaltStrike_Sleep_Decoder_Indicator, Description: Detects CobaltStrike sleep_mask decoder, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: HKTL_CobaltStrike_SleepMask_Jul22, Description: Detects static bytes in Cobalt Strike 4.5 sleep mask function that are not obfuscated, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: CodeX • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike, Description: Yara detected CobaltStrike, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_CobaltStrike_ee756db7, Description: Attempts to detect Cobalt Strike based on strings found in BEACON, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_663fc95d, Description: Identifies CobaltStrike via unidentified function code, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_b54b94ac, Description: Rule for beacon sleep obfuscation routine, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000003.00000002.708528999.0000025BF8AB0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Cobaltbaltstrike_Beacon_Encoded, Description: Detects CobaltStrike payloads, Source: 00000003.00000002.706488711.000000C00023E000.00000004.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: HKTL_Meterpreter_inMemory, Description: Detects Meterpreter in-memory, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: netbiosX, Florian Roth • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: Cobaltbaltstrike_Beacon_x64, Description: Detects CobaltStrike payloads, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltStrike_Sleep_Decoder_Indicator, Description: Detects CobaltStrike sleep_mask decoder, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: CobaltStrike_MZ_Launcher, Description: Detects CobaltStrike MZ header ReflectiveLoader launcher, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: HKTL_CobaltStrike_SleepMask_Jul22, Description: Detects static bytes in Cobalt Strike 4.5 sleep mask function that are not obfuscated, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: CodeX • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key., Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_4, Description: Yara detected CobaltStrike, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike, Description: Yara detected CobaltStrike, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_CobaltStrike_ee756db7, Description: Attempts to detect Cobalt Strike based on strings found in BEACON, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_663fc95d, Description: Identifies CobaltStrike via unidentified function code, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_b54b94ac, Description: Rule for beacon sleep obfuscation routine, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000003.00000002.706659139.000000C000294000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: HKTL_Meterpreter_inMemory, Description: Detects Meterpreter in-memory, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: netbiosX, Florian Roth • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: Cobaltbaltstrike_Beacon_x64, Description: Detects CobaltStrike payloads, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltStrike_Sleep_Decoder_Indicator, Description: Detects CobaltStrike sleep_mask decoder, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: CobaltStrike_MZ_Launcher, Description: Detects CobaltStrike MZ header ReflectiveLoader launcher, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: HKTL_CobaltStrike_SleepMask_Jul22, Description: Detects static bytes in Cobalt Strike 4.5 sleep mask function that are not obfuscated, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: CodeX • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key., Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

	• Rule: JoeSecurity_CobaltStrike_4, Description: Yara detected CobaltStrike, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike, Description: Yara detected CobaltStrike, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_CobaltStrike_ee756db7, Description: Attempts to detect Cobalt Strike based on strings found in BEACON, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_663fc95d, Description: Identifies CobaltStrike via unidentified function code, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_b54b94ac, Description: Rule for beacon sleep obfuscation routine, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000003.00000002.708356136.0000025BF8A60000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 26%, Metadefender, Browse • Detection: 62%, ReversingLabs
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

Analysis Process: conhost.exe PID: 5860, Parent PID: 3016

General

Target ID:	4
Start time:	09:55:47
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5788, Parent PID: 5296

General

Target ID:	5
Start time:	09:55:47
Start date:	05/08/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c start ??????????????????????.docx
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: conhost.exe PID: **2164**, Parent PID: **5788**

General

Target ID:	6
Start time:	09:55:48
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WINWORD.EXE PID: **5308**, Parent PID: **5788**

General

Target ID:	7
Start time:	09:55:49
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n "C:\Users\user\Desktop\??????????????????????.docx" /o "
Imagebase:	0xb60000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly