ID: 329945
Sample Name: v1Us5AICBm
Cookbook: default.jbs
Time: 17:59:10
Date: 13/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

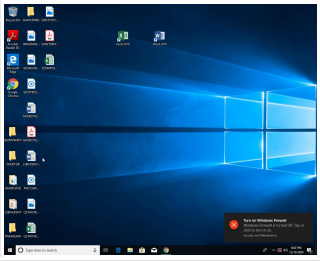
Analysis Report v1Us5AICBm

Overview

General Information

Sample Name:	v1Us5AICBm (renamed file extension from none to dll)
Analysis ID:	329945
MD5:	e0af3054669d623.
SHA1:	f0aa6e50471e70d.
SHA256:	f8503947e0e9848.
Tags:	zloader2

Most interesting Screenshot:



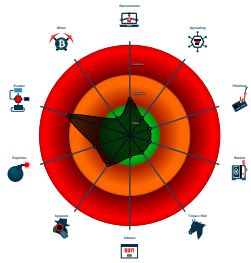
Detection

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Contains functionality to inject code …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Abnormal high CPU Usage
- Antivirus or Machine Learning detec…
- Contains functionality to check the p…
- Contains functionality to dynamically…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function
- Drops PE files

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5312 cmdline: loaddll32.exe 'C:\Users\user\Desktop\v1Us5AICBm.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - msiexec.exe (PID: 6160 cmdline: msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

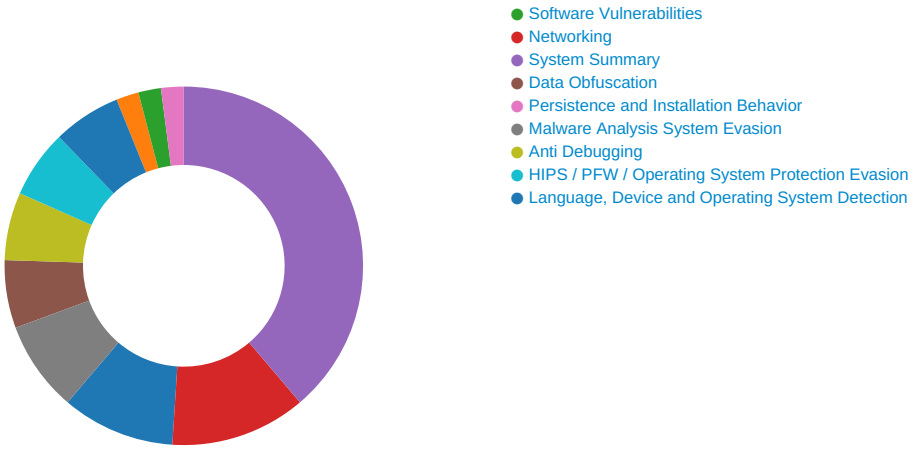
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Spreading



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

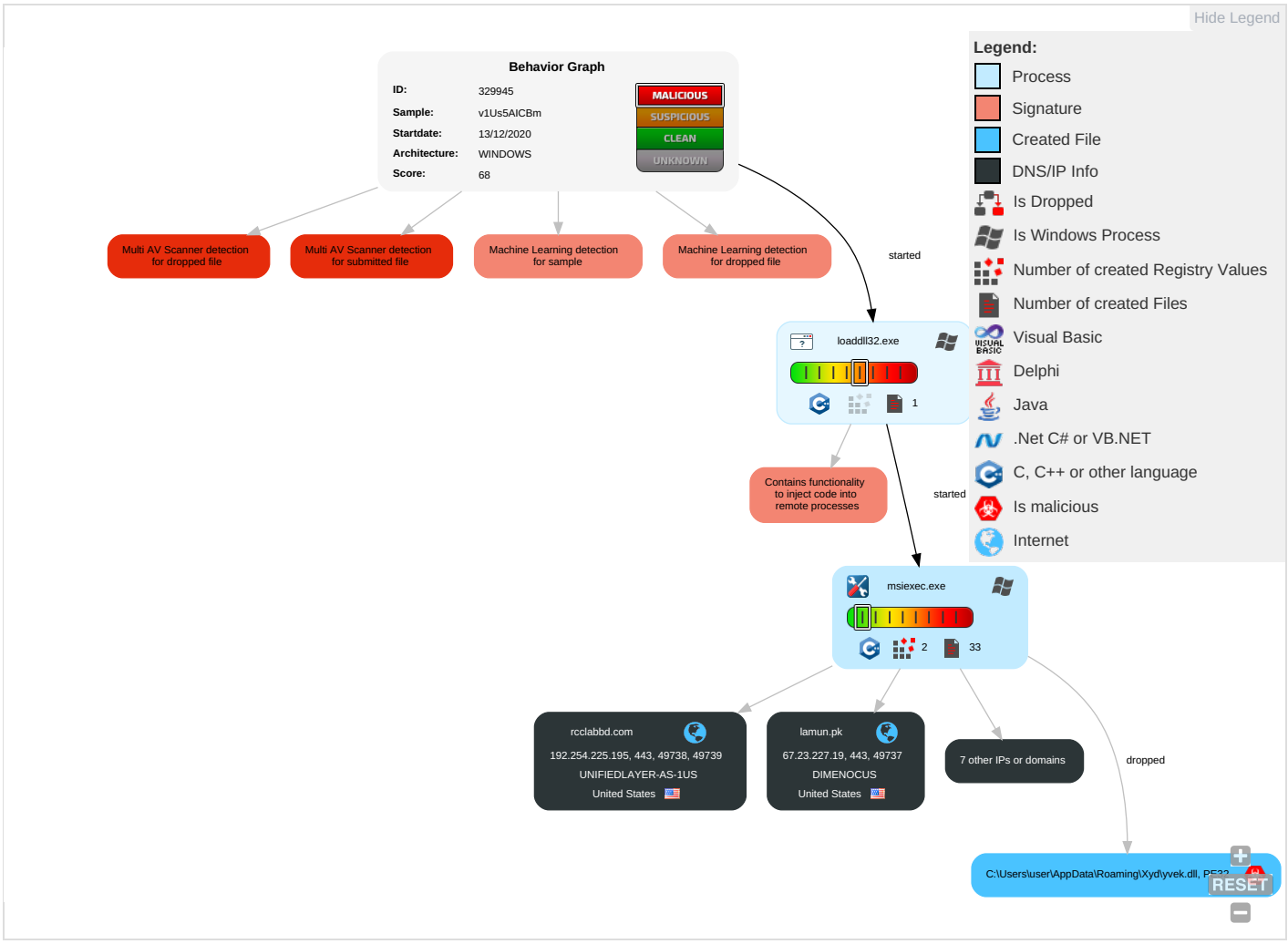
HIPS / PFW / Operating System Protection Evasion:

Contains functionality to inject code into remote processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remo Servi Effec
Valid Accounts	Native API 1	DLL Side-Loading 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Remo Track Witho Autho
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Access Token Manipulation 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Autho
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Process Injection 1 1 2	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtai Devic Cloud Backu
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 3	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

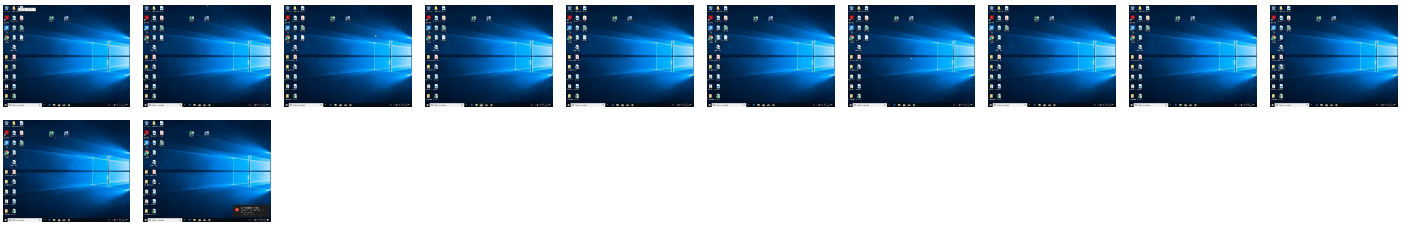
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
v1Us5AICBm.dll	47%	Virustotal		Browse
v1Us5AICBm.dll	28%	ReversingLabs	Win32.Trojan.Generic	
v1Us5AICBm.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Xyd\yvek.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Xyd\yvek.dll	28%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
12.2.msiexec.exe.350000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
squire.ae	2%	Virustotal		Browse
lamun.pk	2%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
rcclabbd.com	0%	Virustotal		Browse
businessinsurancelaw.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://thecype.com/wp-punch.phpefaults	0%	Avira URL Cloud	safe	
http://apps.ident	0%	Avira URL Cloud	safe	
http://crt.comodoca.o	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.rcclabbd.com/wp-punch.phpr	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://thetertеboltallbrow.tk/f	0%	Avira URL Cloud	safe	
http://https://www.businessinsurancelaw.com/wp-punch.phpVe	0%	Avira URL Cloud	safe	
http://https://thetertеboltallbrow.tk/j	0%	Avira URL Cloud	safe	
http://ocsp.comodoca.cog	0%	Avira URL Cloud	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://https://www.rcclabbd.com/wp-punch.php;	0%	Avira URL Cloud	safe	
http://https://lamun.pk/	0%	Avira URL Cloud	safe	
http://https://thetertеboltallbrow.tk/wp-smarts.phpSNfc)	0%	Avira URL Cloud	safe	
http://https://thetertеboltallbrow.tk/	0%	Avira URL Cloud	safe	
http://https://squire.ae/wp-punch.php?	0%	Avira URL Cloud	safe	
http://https://www.businessinsurancelaw.com/wp-punch.php	0%	Avira URL Cloud	safe	
http://https://lamun.pk/R	0%	Avira URL Cloud	safe	
http://https://thecype.com/	0%	Avira URL Cloud	safe	
http://https://thetertеboltallbrow.tk/;	0%	Avira URL Cloud	safe	
http://https://www.businessinsurancelaw.com/wp-punch.php(	0%	Avira URL Cloud	safe	
http://https://thecype.com/wp-punch.php)	0%	Avira URL Cloud	safe	
http://https://thetertеboltallbrow.tk/wp-smarts.php;	0%	Avira URL Cloud	safe	
http://https://thetertеboltallbrow.tk/wp-smarts.php	0%	Avira URL Cloud	safe	
http://https://www.rcclabbd.com/crosoft	0%	Avira URL Cloud	safe	
http://https://lamun.pk/wp-punch.php	0%	Avira URL Cloud	safe	
http://https://lamun.pk/wp-punch.phpc	0%	Avira URL Cloud	safe	
http://https://squire.ae/	0%	Avira URL Cloud	safe	
http://https://lamun.pk/wp-punch.phpT%	0%	Avira URL Cloud	safe	
http://https://www.rcclabbd.com/z#	0%	Avira URL Cloud	safe	
http://https://www.rcclabbd.com/wp-punch.php	0%	Avira URL Cloud	safe	
http://https://www.rcclabbd.com/	0%	Avira URL Cloud	safe	
http://crl.co	0%	Avira URL Cloud	safe	
http://https://lamun.pk/wp-punch.php(	0%	Avira URL Cloud	safe	
http://https://www.businessinsurancelaw.com/	0%	Avira URL Cloud	safe	
http://https://squire.ae/wp-punch.php	0%	Avira URL Cloud	safe	
http://https://www.rcclabbd.com/wp-punch.phpH	0%	Avira URL Cloud	safe	
http://https://thetertеboltallbrow.tk/wp-smarts.phpider	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.ro	0%	Avira URL Cloud	safe	
http://https://thecype.com/wp-punch.php	0%	Avira URL Cloud	safe	
http://https://www.businessinsurancelaw.com/wp-punch.phptw	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

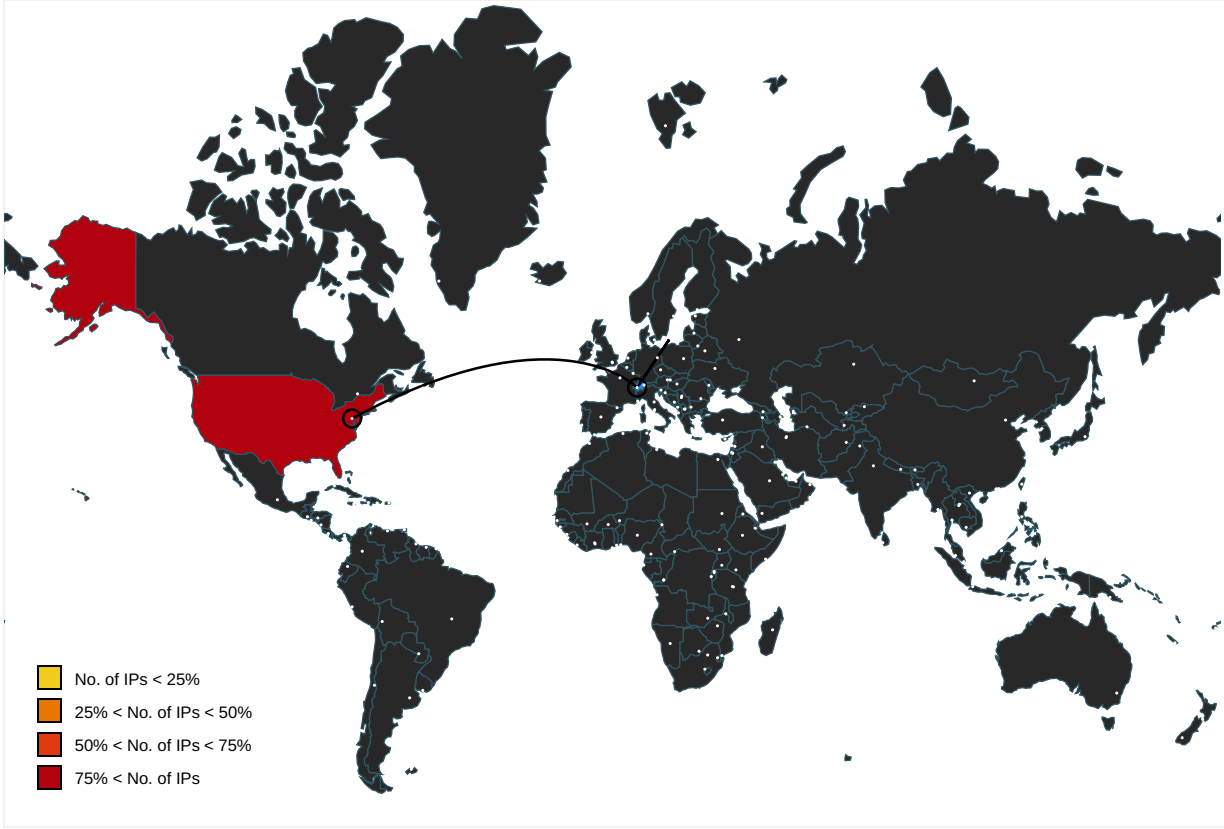
Name	IP	Active	Malicious	Antivirus Detection	Reputation
squire.ae	70.32.23.56	true	false	• 2%, Virustotal, Browse	unknown
lamun.pk	67.23.227.19	true	false	• 2%, Virustotal, Browse	unknown
rcclabbd.com	192.254.225.195	true	false	• 0%, Virustotal, Browse	unknown
businessinsurancelaw.com	70.32.23.56	true	false	• 1%, Virustotal, Browse	unknown
thecype.com	192.3.183.226	true	false		unknown
www.businessinsurancelaw.com	unknown	unknown	false		unknown
theterteboltallbrow.tk	unknown	unknown	false		unknown
www.rcclabbd.com	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://thecype.com/wp-punch.phpefaults	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://apps.ident	msiexec.exe, 0000000C.00000003.339000834.0000000000957000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.comodoca.o	msiexec.exe, 0000000C.00000003.306019326.0000000000938000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.rcclabbd.com/wp-punch.phpr	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	msiexec.exe, 0000000C.00000003.337005926.0000000000963000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://thetertеboltallbrow.tk/f	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.businessinsurancelaw.com/wp-punch.phpVe	msiexec.exe, 0000000C.00000003.303659662.0000000000909000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://thetertеboltallbrow.tk/j	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.comodoca.cog	msiexec.exe, 0000000C.00000003.306019326.0000000000938000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.int-x3.letsencrypt.org0/	msiexec.exe, 0000000C.00000003.337005926.0000000000963000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.rcclabbd.com/wp-punch.php;	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lamun.pk/	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://thetertеboltallbrow.tk/wp-smarts.phpSNfc)	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://thetertеboltallbrow.tk/	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://squire.ae/wp-punch.php?	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.businessinsurancelaw.com/wp-punch.php	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lamun.pk/R	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://thecype.com/	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://thetertеboltallbrow.tk/;	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.businessinsurancelaw.com/wp-punch.php(	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://thecype.com/wp-punch.php)	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://theterteboltallbrow.tk/wp-smarts.php;	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://theterteboltallbrow.tk/wp-smarts.php	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp, msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.rcclabbd.com/crosoft	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lamun.pk/wp-punch.php	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lamun.pk/wp-punch.phpc	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://squire.ae/	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lamun.pk/wp-punch.phpT%	msiexec.exe, 0000000C.00000003.308169882.0000000000938000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.rcclabbd.com/z#	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://cert.int-x3.letsencrypt.org/0	msiexec.exe, 0000000C.00000003.337005926.0000000000963000.00000004.00000001.sdmp	false		high
http://https://www.rcclabbd.com/wp-punch.php	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://theterteboltallbrow.tk/J	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false		unknown
http://https://www.rcclabbd.com/	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.co	msiexec.exe, 0000000C.00000003.306019326.0000000000938000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lamun.pk/wp-punch.php(	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.businessinsurancelaw.com/	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://squire.ae/wp-punch.php	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.rcclabbd.com/wp-punch.phpH	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://theterteboltallbrow.tk/wp-smarts.phpider	msiexec.exe, 0000000C.00000002.565639783.000000000091B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	msiexec.exe, 0000000C.00000003.337005926.0000000000963000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.ro	msiexec.exe, 0000000C.00000003.339000834.0000000000957000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://thecype.com/wp-punch.php	msiexec.exe, 0000000C.00000002.565307219.00000000008C8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.businessinsurancelaw.com/wp-punch.phptw	msiexec.exe, 0000000C.00000003.303659662.0000000000909000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.254.225.195	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
192.3.183.226	unknown	United States		36352	AS-COLOCROSSINGUS	false
70.32.23.56	unknown	United States		55293	A2HOSTINGUS	false
67.23.227.19	unknown	United States		33182	DIMENOCUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	329945
Start date:	13.12.2020
Start time:	17:59:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	v1Us5AICBm (renamed file extension from none to dll)
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:	mal68.evad.winDLL@3/1@11/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 70.9% (good quality ratio 70.4%) • Quality average: 88.9% • Quality standard deviation: 20.1%
HCA Information:	• Successful, ratio: 63% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 40.88.32.150, 51.104.139.180, 23.210.248.85, 8.253.95.121, 67.27.157.254, 8.248.147.254, 67.27.157.126, 67.27.233.126, 20.54.26.129, 92.122.213.194, 92.122.213.247, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.254.225.195	wp-scan.dll	Get hash	malicious	Browse	
192.3.183.226	wp-scan.dll	Get hash	malicious	Browse	
	http://https://www.nonnie.com.ng/ruis?email=kymo@willowoodusa.com	Get hash	malicious	Browse	
	http://https://nam03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fspecfrial.online%2Fc2890d44d06bafb6c7b4aa194857ccbc%3Fid%3DbWFyay5iYXVtYW5Ab3dlbnNjb3JuaW5nLmNvbQ%3D%3D&data=02%7C01%7CPaul.Townley%40owenscorning.com%7C57e80c6031f94a765cd708d6a63fe7ef%7C09e4e683c8e44a8095d37f078d5a2649%7C0%7C0%7C636879190739673644&sdata=t4aWtIJoLI5bTvAlkH9b%2FIN7y6GseWVQVCGNqaSF2C4%3D&reserved=0	Get hash	malicious	Browse	
	http://https://odresfua.online/ce93b7b0e618ad3ba298514c691dfad1?email=YmlyZGllLmNob3dAYWR2b2NhdGVoZWFsdGguY29t	Get hash	malicious	Browse	
70.32.23.56	wp-scan.dll	Get hash	malicious	Browse	
	doc.5756.xls	Get hash	malicious	Browse	
	Ord5967.xls	Get hash	malicious	Browse	
	invoice907.xls	Get hash	malicious	Browse	
	Doc-7679.xls	Get hash	malicious	Browse	
	order_1405.xls	Get hash	malicious	Browse	
	http://https://shell-core.com/j2aqm0xkt.rar	Get hash	malicious	Browse	
67.23.227.19	wp-scan.dll	Get hash	malicious	Browse	
	_#Ud83d#Udcde953@Westerntrust.hscni.net.htm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
thecype.com	wp-scan.dll	Get hash	malicious	Browse	• 192.3.183.226
lamun.pk	wp-scan.dll	Get hash	malicious	Browse	• 67.23.227.19
squire.ae	wp-scan.dll	Get hash	malicious	Browse	• 70.32.23.56

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	aG2hS5oQsq.exe	Get hash	malicious	Browse	• 162.241.60.214
	3W9Z5Mn6Nh.rtf	Get hash	malicious	Browse	• 108.179.243.169
	DGkPaXmPUx.rtf	Get hash	malicious	Browse	• 192.185.129.64
	wp-scan.dll	Get hash	malicious	Browse	• 192.254.225.195
	SWIFT-MTC749892-10-12-20_pdf.exe	Get hash	malicious	Browse	• 192.185.216.110
	SN-17-2020.pdf.exe	Get hash	malicious	Browse	• 192.185.216.110
	Purchase Order#12202011.exe	Get hash	malicious	Browse	• 50.87.195.38
	http://https://timcoulson.com/mailer-daemon/?mail=james.dean@ahtd.ar.gov	Get hash	malicious	Browse	• 162.241.219.35
	http://https://sneakyveggies.com/wp-add	Get hash	malicious	Browse	• 162.241.124.195
	http://https://preventivahealth.com/document.html	Get hash	malicious	Browse	• 192.185.79.175
	http://https://morelifedrop.net/CD/office365.htm	Get hash	malicious	Browse	• 162.241.127.85
	http://amar.alwani.xalia-outlet.com/exr/amar.alwani@centrica.com	Get hash	malicious	Browse	• 69.49.228.190
	http://https://studntnu-my.sharepoint.com/:o:/g/personal/kirkebyg_ntnu_no/Eibio0jRkINJtrQ2cGW93HsBV-2OJ7plGr0_fP6Yhp0ZKw?e=zzCFN4	Get hash	malicious	Browse	• 162.241.27.46
	http://https://apcel-my.sharepoint.com/:o:/g/personal/mats_bjarnlid_apcel_se/Eo9dNcg7tRlLmRjiyE3DcEsBUUdhzATanbO-fWy_MABjEw?e=SGCxVg	Get hash	malicious	Browse	• 162.241.27.46
	http://https://statuscollectionuniform.com/wp-admin/AU/masterlifts/Global/Projects/Share/index.php	Get hash	malicious	Browse	• 162.214.75.114
	http://https://sangal.com.mx/.outlook.html	Get hash	malicious	Browse	• 192.185.131.183
	Payment Advice Notification.xlsx	Get hash	malicious	Browse	• 50.87.153.159
	Payment Advice Notification.xlsx	Get hash	malicious	Browse	• 50.87.153.159
	Payment Advice Notification.xlsx	Get hash	malicious	Browse	• 50.87.153.159
	Payment Advice Notification.xlsx	Get hash	malicious	Browse	• 50.87.153.159
A2HOSTINGUS	pty4	Get hash	malicious	Browse	• 162.249.2.189
	wp-scan.dll	Get hash	malicious	Browse	• 70.32.23.56

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://shimypurr.com/asf/Twadle/00698/dHdhZGxlQHZlcm1lZXIuY29t	Get hash	malicious	Browse	• 67.209.121.100
	pty3	Get hash	malicious	Browse	• 68.66.253.100
	doc.5756.xls	Get hash	malicious	Browse	• 70.32.23.56
	output.xls	Get hash	malicious	Browse	• 70.32.23.16
	output.xls	Get hash	malicious	Browse	• 70.32.23.16
	output.xls	Get hash	malicious	Browse	• 70.32.23.16
	Ord5967.xls	Get hash	malicious	Browse	• 70.32.23.56
	invoice907.xls	Get hash	malicious	Browse	• 70.32.23.56
	Doc-7679.xls	Get hash	malicious	Browse	• 70.32.23.56
	order_1405.xls	Get hash	malicious	Browse	• 70.32.23.56
	Order.862393485.doc	Get hash	malicious	Browse	• 66.198.240.31
	http://https://shell-core.com/j2aqm0xkt.rar	Get hash	malicious	Browse	• 70.32.23.56
	http://secure-file-transfer-ver.webflow.io	Get hash	malicious	Browse	• 68.66.216.57
	http://https://teams-securelink-flow-docs.webflow.io/	Get hash	malicious	Browse	• 68.66.216.57
	http://https://globalforwarding.com.pe/Maersk/Maersk_line-delivery.php?code=63926583659	Get hash	malicious	Browse	• 68.66.226.79
	Fdquqwatjjr.exe	Get hash	malicious	Browse	• 85.187.154.178
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 85.187.154.178
	Purchase Order.exe	Get hash	malicious	Browse	• 85.187.154.178
AS-COLOCROSSINGUS	Quotation No. 233.xlsx	Get hash	malicious	Browse	• 192.3.146.192
	DEC 12-10 Wires.xlsx	Get hash	malicious	Browse	• 192.3.22.9
	TT 18,000.00 euro.xlsx	Get hash	malicious	Browse	• 216.170.126.121
	NEW PO-TRUSTC20-0604.exe	Get hash	malicious	Browse	• 154.16.116.113
	wp-scan.dll	Get hash	malicious	Browse	• 192.3.183.226
	ORDER.xlsx	Get hash	malicious	Browse	• 216.170.126.121
	101220b64.exe	Get hash	malicious	Browse	• 192.3.247.106
	3166805_Invoice_Receipt.exe	Get hash	malicious	Browse	• 198.12.123.178
	PreviewDoc.exe	Get hash	malicious	Browse	• 192.3.247.106
	Print-Review.exe	Get hash	malicious	Browse	• 192.3.247.106
	Print-Review.exe	Get hash	malicious	Browse	• 192.3.247.106
	New Order list.xlsx	Get hash	malicious	Browse	• 75.127.1.225
	HEMANI GROUP NEW ORDER.xlsx	Get hash	malicious	Browse	• 216.170.114.70
	d84S4fxGCp.doc	Get hash	malicious	Browse	• 198.12.123.178
	RRC-095-20.xlsx	Get hash	malicious	Browse	• 192.3.146.194
	Material Requisition and Order.xlsx	Get hash	malicious	Browse	• 192.3.146.169
	Shipping_Docs 12-09.xlsx	Get hash	malicious	Browse	• 198.12.125.17
	NewOrder-98542009.xlsx	Get hash	malicious	Browse	• 198.23.213.32
	PO2932.xlsx	Get hash	malicious	Browse	• 192.3.146.171
	TOo0haekwZ.exe	Get hash	malicious	Browse	• 198.12.125.17
DIMENOCUS	wp-scan.dll	Get hash	malicious	Browse	• 67.23.227.19
	http://https://onlinegenera.sn.am/lZnJUY4u40q	Get hash	malicious	Browse	• 67.23.232.130
	http://https://onlinegenera.sn.am/lZnJUY4u40q	Get hash	malicious	Browse	• 67.23.232.130
	http://https://onlinegenera.sn.am/lZnJUY4u40q	Get hash	malicious	Browse	• 67.23.232.130
	Order.862393485.doc	Get hash	malicious	Browse	• 184.171.251.122
	Payment form-976107909.doc	Get hash	malicious	Browse	• 184.171.251.122
	DOC051220-007_pdf.exe	Get hash	malicious	Browse	• 199.168.190.42
	Remittance.exe	Get hash	malicious	Browse	• 67.23.254.42
	i_Remittance.exe	Get hash	malicious	Browse	• 67.23.254.42
	vale-remittance.exe	Get hash	malicious	Browse	• 67.23.254.42
	_#Ud83d#Udcde953@Westerntrust.hscni.net.htm	Get hash	malicious	Browse	• 67.23.227.19
	http://https://h2oholdings.lk/smskod/one/westpac/login	Get hash	malicious	Browse	• 107.161.181.250
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 67.23.238.50
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 67.23.238.50
	http://250374-5014.futureriseeducation.com/qhlpbczkwxve/dG9tLndpbGN6YWtAc2VhcnNoYy5jb20=	Get hash	malicious	Browse	• 67.23.242.106
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	• 198.136.51.123
	http://www.947947.mirramodaintima.com.br/#aHR0cHM6Ly9lbXl0dXJrLmNvbS9zZC9JSy9vZjEvRmlkZWwuVG9ycmVzQHNlYXJzaGMuY29t	Get hash	malicious	Browse	• 177.234.159.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	invoice.exe	Get hash	malicious	Browse	• 109.73.164.114
	ddos_____ (IW0Irt2zSey6D6LMEgcs2kqQiSuMa 8 G).js	Get hash	malicious	Browse	• 67.23.238.50
	ddos_____ (IW0Irt2zSey6D6LMEgcs2kqQiSuMa 8 G).js	Get hash	malicious	Browse	• 67.23.238.50

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Ca4fOzoNzJ.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	FAEROE#U007e0.EXE	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	VITHAF#U007e0.EXE	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	U0N4EBAJKJ.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	DAK0SFLsXV.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	TrustedInstaller.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	wp-scan.dll	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	SWIFT-MTC749892-10-12-20_pdf.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	aPe6wtn4Y8.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	Pw5WhqWFzK.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	soft.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	SN-17-2020.pdf.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	MSI4614.dll	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	zethpill.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	imgengine.dll	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	http://email.dream11.com/ls/click?upn=gIaedBDL7lfVNdbAB8knTqzWOtzKjiGAdIjxItTBzfisZ9eaHsszPGYIVZ5c9tVbThEq-2F7r5H1ddfXxGAiqSEA-3D-3Dy1dA_TJcqyuN2iNYyC7hiQE8uPnpIrwAwiFHKa7P9O3CiGRV5Zdc60yh-2FWLCKsCnUSROY-2BBKuKVdEC0LWtK4-2FOrxpuEIEn6IxtcLH08KwUXmYODW9pymsy9zpjJC1l0k2-2B2ZGDA7llrlg-2BDC-2Fg3YTrgVq0OyM4w1U-2FU2mGIUK7D9YLK8POQedJhTmuBqzj8PIDSm2-2Bu5mOV-2B6GOLE63z6lg4PTw-3D-3D	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	http://https://intouch.mtn.com	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	http://https://nelleinletapt.buzz/CD/office365.htm	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fin0038847990.sn.am%2flfCk7ZE6GWq&c=E,1,XbwqZlmKwFAf_trFhDdV9wkuU6vutPEIQqN4IhE8jUbxLD3wnPPXDvKp8Jibjk9HngPAI5iRQWnG4vU_DQMKfMGkzgCqkZ-4BfRprMNSl9Nr7VoPQEtWNft5&typo=1	Get hash	malicious	Browse	• 192.254.225.195 • 192.3.183.226 • 70.32.23.56 • 67.23.227.19

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\Xyd\yvek.dll

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	389120
Entropy (8bit):	6.772300701631193
Encrypted:	false
SSDEEP:	6144:j2yIqOCYbeyUaNpV55IQB5ykPgScnOfIvI+ZcZfqAf7Vv7U0+jG8CuJ:jPYb3UaNpV52QB5ykXcqacZfqARv7Bmj
MD5:	E0AF3054669D6232870B87E1E239A689
SHA1:	F0AA6E50471E70D07A1B70207F38538CB31ED569
SHA-256:	F8503947E0E984865A29D1E3F8A62CE7034069F49C2A2DD902AF68274F192224
SHA-512:	1574E2ACA2415A90677053DA5F625D4A9E3BB2E85362CC7ACC7B6430A35EB889883DA1FDA694D79EE38349FEE01B5843D0717D864E2D801302755188308D513F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=B..S...S...S.[(-...S..*>...S..*....S..*(...S..*=...S.....S...R.+.S..*!...S..*)...S..*/...S..*+...S.Rich..S.....PE..L....6}E.....!.....P.....&.....`.....h...x....0.....@..... .....{..@.....text...(..... ..`.rdata.....@..@.data..... .....@....rsrc.....0.....@..@.reloc.....@... .....@..B.....

Static File Info

General

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.772300701631193
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	v1Us5AICBm.dll
File size:	389120
MD5:	e0af3054669d6232870b87e1e239a689
SHA1:	f0aa6e50471e70d07a1b70207f38538cb31ed569
SHA256:	f8503947e0e984865a29d1e3f8a62ce7034069f49c2a2dd902af68274f192224
SHA512:	1574e2aca2415a90677053da5f625d4a9e3bb2e85362cc7acc7b6430a35eb889883da1fda694d79ee38349fee01b5843d0717d864e2d801302755188308d513f
SSDEEP:	6144:j2yIqOCYbeyUaNpV55IQB5ykPgScnOfIvI+ZcZfqAf7Vv7U0+jG8CuJ:jPYb3UaNpV52QB5ykXcqacZfqARv7Bmj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=B..S...S...S.[(-...S..*>...S..*....S..*(...S..*=...S.....S...R.+.S..*!...S..*)...S..*/...S..*+...S.Rich..S.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100026e5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x457D36C4 [Mon Dec 11 10:45:24 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ac30ec1b90a9fedffe3cfc3e897b5a40

Entrypoint Preview

Instruction
cmp dword ptr [esp+08h], 01h
jne 00007F0A38FE5CE7h
call 00007F0A38FEAD5Ah
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
call 00007F0A38FE5BD2h
pop ecx
retn 000Ch
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F0A38FE5D06h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F0A38FE5D30h
test ecx, 00000003h
jne 00007F0A38FE5CD1h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F0A38FE5CCAh
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F0A38FE5D14h
test ah, ah
je 00007F0A38FE5D06h
test eax, 00FF0000h
je 00007F0A38FE5CF5h
test eax, FF000000h
je 00007F0A38FE5CE4h
jmp 00007F0A38FE5CAFh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 000512D0h

Rich Headers

Programming Language:	• [RES] VS2005 build 50727 • [C] VS2005 build 50727 • [EXP] VS2005 build 50727 • [IMP] VS2005 build 50727 • [C++] VS2005 build 50727 • [ASM] VS2005 build 50727 • [LNK] VS2005 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x58568	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x63000	0xf80	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x64000	0x11b0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x51220	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	0x57bf8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x51000	0x1e0	.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	0x4fb28	0x50000	False	0.811544799805	data	6.97945124569	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x51000	0x800c	0x9000	False	0.459689670139	data	5.7180496081	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5a000	0x87f8	0x2000	False	0.2216796875	data	2.42882006124	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x63000	0xf80	0x1000	False	0.371826171875	data	3.49422984211	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x64000	0x1f06	0x2000	False	0.472290039062	data	4.57666635881	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x63588	0xcc	data	English	United States
RT_DIALOG	0x63658	0xc0	data	English	United States
RT_DIALOG	0x63718	0xbc	data	English	United States
RT_DIALOG	0x637d8	0x148	data	English	United States
RT_DIALOG	0x63920	0xd0	data	English	United States
RT_DIALOG	0x639f0	0x140	data	English	United States
RT_DIALOG	0x63b30	0xc8	data	English	United States
RT_DIALOG	0x63bf8	0x142	data	English	United States
RT_DIALOG	0x63d40	0xbc	data	English	United States
RT_VERSION	0x63270	0x318	data	English	United States
RT_MANIFEST	0x63e00	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	LCMapStringW, VirtualProtect, GetStringTypeA, HeapReAlloc, GetStringTypeW, GetCurrentThreadId, GetLocaleInfoA, HeapSize, LoadLibraryA, InitializeCriticalSection, CompareStringA, CompareStringW, GetVersion, WriteFile, FindFirstChangeNotificationA, GetDiskFreeSpaceA, RemoveDirectoryA, CreateProcessA, CreateEventA, LCMapStringA, Sleep, GetSystemTimeAsFileTime, GetCommandLineA, HeapFree, GetVersionExA, HeapAlloc, GetProcessHeap, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetLastError, GetCPInfo, InterlockedIncrement, InterlockedDecrement, GetACP, GetOEMCP, GetProcAddress, GetModuleHandleA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, MultiByteToWideChar, GetTimeFormatA, GetDateFormatA, WideCharToMultiByte, GetTimeZoneInformation, ExitProcess, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapDestroy, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, LeaveCriticalSection, EnterCriticalSection, VirtualAlloc, SetEnvironmentVariableA
USER32.dll	GetMessageA, CloseClipboard, GetClassNameA, MapDialogRect, LoadIconA, SetParent, ExitWindowsEx, GetDC, InflateRect, OffsetRect, GetWindowTextA, GetAsyncKeyState, IntersectRect, EndDialog, EnumChildWindows, UpdateWindow, FindWindowA, EndDeferWindowPos, GetMessagePos
GDI32.dll	SetTextColor, SetBkColor, SetAbortProc, CreateBitmap, SetRectRgn, CombineRgn, StretchDIBits, GetClipBox, GetTextMetricsA, AbortDoc, EndDoc
COMDLG32.dll	CommDlgExtendedError, GetOpenFileNameA, GetSaveFileNameA, GetFileTitleA, ChooseFontA, ReplaceTextA
COMCTL32.dll	ImageList_Remove, InitCommonControlsEx, ImageList_SetBkColor, ImageList_SetIconSize, ImageList_Destroy, ImageList_SetDragCursorImage

Version Infos

Description	Data
LegalCopyright	Figskin Corporation. All rights reserved
InternalName	Pound Bit
FileVersion	8.3.0.634
CompanyName	Figskin Corporation
ProductName	Figskin Scienceland
ProductVersion	8.3.0.634
FileDescription	Figskin Scienceland
OriginalFilename	hole.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 78

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 18:00:44.319030046 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.445207119 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:44.445550919 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.496025085 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.623572111 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:44.623622894 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:44.623661041 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:44.623702049 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:44.623739958 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:44.623748064 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.623790026 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.623796940 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.623801947 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.740991116 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.867456913 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:44.867938042 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:44.900187969 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.065598965 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.370954037 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.370989084 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.371026039 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.371112108 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.371161938 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.371515036 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.371678114 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.498420954 CET	443	49735	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.498591900 CET	49735	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.621951103 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.748013020 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.748150110 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.748992920 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.874871969 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.876118898 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.876140118 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.876154900 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.876168966 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:45.876434088 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:45.903753996 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.030296087 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:46.030777931 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.032215118 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.197670937 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:46.478622913 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:46.478667974 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:46.478696108 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:46.478775024 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.478825092 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.478832006 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.478863001 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.478935957 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.591269016 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:46.604706049 CET	443	49736	70.32.23.56	192.168.2.3
Dec 13, 2020 18:00:46.604835033 CET	49736	443	192.168.2.3	70.32.23.56
Dec 13, 2020 18:00:46.718322039 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:46.718473911 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:46.726059914 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:46.853110075 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:46.854614973 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:46.854670048 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:46.854700089 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:46.854820967 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:46.854866028 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:46.869280100 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:46.996562004 CET	443	49737	67.23.227.19	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 18:00:46.996750116 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:46.997703075 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:47.164597034 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:47.503226995 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:47.503273010 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:47.503510952 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:47.503592014 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:47.503647089 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:47.503796101 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:47.503871918 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:47.630857944 CET	443	49737	67.23.227.19	192.168.2.3
Dec 13, 2020 18:00:47.631016016 CET	49737	443	192.168.2.3	67.23.227.19
Dec 13, 2020 18:00:47.727953911 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:47.886188030 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:47.887159109 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:47.889065981 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.047314882 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.050368071 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.050420046 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.050462008 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.050683022 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.077200890 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.236044884 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.236316919 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.237912893 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.406014919 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.406060934 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.406089067 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.406157017 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.406202078 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.406461000 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.406522989 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.424137115 CET	49739	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.564574957 CET	443	49738	192.254.225.195	192.168.2.3
Dec 13, 2020 18:00:48.564666986 CET	49738	443	192.168.2.3	192.254.225.195
Dec 13, 2020 18:00:48.582658052 CET	443	49739	192.254.225.195	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 17:59:52.110733032 CET	53195	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:52.134998083 CET	53	53195	8.8.8.8	192.168.2.3
Dec 13, 2020 17:59:53.136502028 CET	50141	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:53.161084890 CET	53	50141	8.8.8.8	192.168.2.3
Dec 13, 2020 17:59:53.969039917 CET	53023	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:53.996448040 CET	53	53023	8.8.8.8	192.168.2.3
Dec 13, 2020 17:59:54.775568962 CET	49563	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:54.799938917 CET	53	49563	8.8.8.8	192.168.2.3
Dec 13, 2020 17:59:55.968637943 CET	51352	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:55.995690107 CET	53	51352	8.8.8.8	192.168.2.3
Dec 13, 2020 17:59:57.135420084 CET	59349	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:57.159847021 CET	53	59349	8.8.8.8	192.168.2.3
Dec 13, 2020 17:59:57.871728897 CET	57084	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:57.899000883 CET	53	57084	8.8.8.8	192.168.2.3
Dec 13, 2020 17:59:58.493649006 CET	58823	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:58.518022060 CET	53	58823	8.8.8.8	192.168.2.3
Dec 13, 2020 17:59:59.518012047 CET	57568	53	192.168.2.3	8.8.8.8
Dec 13, 2020 17:59:59.545289993 CET	53	57568	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:00.191864014 CET	50540	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:00.216548920 CET	53	50540	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:01.227436066 CET	54366	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:01.254662991 CET	53	54366	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:02.154442072 CET	53034	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:02.181777000 CET	53	53034	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2020 18:00:22.572859049 CET	57762	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:22.597362995 CET	53	57762	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:26.736121893 CET	55435	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:26.781519890 CET	53	55435	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:42.112818003 CET	50713	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:42.137171984 CET	53	50713	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:42.501646996 CET	56132	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:42.545161009 CET	53	56132	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:44.156333923 CET	58987	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:44.293592930 CET	53	58987	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:45.447274923 CET	56579	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:45.616791964 CET	53	56579	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:46.527847052 CET	60633	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:46.587399006 CET	53	60633	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:47.556493998 CET	61292	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:47.724914074 CET	53	61292	8.8.8.8	192.168.2.3
Dec 13, 2020 18:00:58.139362097 CET	63619	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:00:58.166681051 CET	53	63619	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:01.057795048 CET	64938	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:01.100646019 CET	53	64938	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:01.960922956 CET	61946	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:02.051309109 CET	53	61946	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:02.058600903 CET	64910	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:02.094324112 CET	53	64910	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:02.180860043 CET	52123	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:02.218029976 CET	53	52123	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:07.111082077 CET	56130	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:07.152836084 CET	53	56130	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:07.160408020 CET	56338	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:07.193361044 CET	53	56338	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:12.204451084 CET	59420	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:12.287242889 CET	53	59420	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:12.304409027 CET	58784	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:12.339963913 CET	53	58784	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:32.026865005 CET	63978	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:32.051188946 CET	53	63978	8.8.8.8	192.168.2.3
Dec 13, 2020 18:01:33.656912088 CET	62938	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:01:33.697693110 CET	53	62938	8.8.8.8	192.168.2.3
Dec 13, 2020 18:02:43.275849104 CET	55708	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:02:43.308525085 CET	53	55708	8.8.8.8	192.168.2.3
Dec 13, 2020 18:02:43.803208113 CET	56803	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:02:43.836067915 CET	53	56803	8.8.8.8	192.168.2.3
Dec 13, 2020 18:02:44.467400074 CET	57145	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:02:44.500171900 CET	53	57145	8.8.8.8	192.168.2.3
Dec 13, 2020 18:02:44.832010031 CET	55359	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:02:44.856794119 CET	53	55359	8.8.8.8	192.168.2.3
Dec 13, 2020 18:02:45.364487886 CET	58306	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:02:45.399610996 CET	53	58306	8.8.8.8	192.168.2.3
Dec 13, 2020 18:02:45.700702906 CET	64124	53	192.168.2.3	8.8.8.8
Dec 13, 2020 18:02:45.728238106 CET	53	64124	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 13, 2020 18:00:44.156333923 CET	192.168.2.3	8.8.8.8	0xca7c	Standard query (0)	www.businessinsurancelaw.com	A (IP address)	IN (0x0001)
Dec 13, 2020 18:00:45.447274923 CET	192.168.2.3	8.8.8.8	0xd7d3	Standard query (0)	squire.ae	A (IP address)	IN (0x0001)
Dec 13, 2020 18:00:46.527847052 CET	192.168.2.3	8.8.8.8	0xa2f1	Standard query (0)	lamun.pk	A (IP address)	IN (0x0001)
Dec 13, 2020 18:00:47.556493998 CET	192.168.2.3	8.8.8.8	0xde36	Standard query (0)	www.rcclabbd.com	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:01.057795048 CET	192.168.2.3	8.8.8.8	0x94b9	Standard query (0)	thecype.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 13, 2020 18:01:01.960922956 CET	192.168.2.3	8.8.8.8	0xb3a0	Standard query (0)	thetertebo ltallbrow.tk	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:02.058600903 CET	192.168.2.3	8.8.8.8	0x7241	Standard query (0)	thetertebo ltallbrow.tk	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:07.111082077 CET	192.168.2.3	8.8.8.8	0xe276	Standard query (0)	thetertebo ltallbrow.tk	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:07.160408020 CET	192.168.2.3	8.8.8.8	0xb92f	Standard query (0)	thetertebo ltallbrow.tk	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:12.204451084 CET	192.168.2.3	8.8.8.8	0xeb0	Standard query (0)	thetertebo ltallbrow.tk	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:12.304409027 CET	192.168.2.3	8.8.8.8	0x79f4	Standard query (0)	thetertebo ltallbrow.tk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 13, 2020 18:00:44.293592930 CET	8.8.8.8	192.168.2.3	0xca7c	No error (0)	www.businessinsurancelaw.com	businessinsurancelaw.com		CNAME (Canonical name)	IN (0x0001)
Dec 13, 2020 18:00:44.293592930 CET	8.8.8.8	192.168.2.3	0xca7c	No error (0)	businessinsurancelaw.com		70.32.23.56	A (IP address)	IN (0x0001)
Dec 13, 2020 18:00:45.616791964 CET	8.8.8.8	192.168.2.3	0xd7d3	No error (0)	squire.ae		70.32.23.56	A (IP address)	IN (0x0001)
Dec 13, 2020 18:00:46.587399006 CET	8.8.8.8	192.168.2.3	0xa2f1	No error (0)	lamun.pk		67.23.227.19	A (IP address)	IN (0x0001)
Dec 13, 2020 18:00:47.724914074 CET	8.8.8.8	192.168.2.3	0xde36	No error (0)	www.rcclabbd.com	rcclabbd.com		CNAME (Canonical name)	IN (0x0001)
Dec 13, 2020 18:00:47.724914074 CET	8.8.8.8	192.168.2.3	0xde36	No error (0)	rcclabbd.com		192.254.225.195	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:01.100646019 CET	8.8.8.8	192.168.2.3	0x94b9	No error (0)	thecype.com		192.3.183.226	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:02.051309109 CET	8.8.8.8	192.168.2.3	0xb3a0	Name error (3)	thetertebo ltallbrow.tk	none	none	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:02.094324112 CET	8.8.8.8	192.168.2.3	0x7241	Name error (3)	thetertebo ltallbrow.tk	none	none	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:07.152836084 CET	8.8.8.8	192.168.2.3	0xe276	Name error (3)	thetertebo ltallbrow.tk	none	none	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:07.193361044 CET	8.8.8.8	192.168.2.3	0xb92f	Name error (3)	thetertebo ltallbrow.tk	none	none	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:12.287242889 CET	8.8.8.8	192.168.2.3	0xeb0	Name error (3)	thetertebo ltallbrow.tk	none	none	A (IP address)	IN (0x0001)
Dec 13, 2020 18:01:12.339963913 CET	8.8.8.8	192.168.2.3	0x79f4	Name error (3)	thetertebo ltallbrow.tk	none	none	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 13, 2020 18:00:44.623739958 CET	70.32.23.56	443	192.168.2.3	49735	CN=businessinsurancelaw.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Sep 29 02:00:00 CEST 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Dec 29 00:59:59 CET 2020 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Dec 13, 2020 18:00:45.876168966 CET	70.32.23.56	443	192.168.2.3	49736	CN=squire.ae CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Oct 29 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jan 28 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Dec 13, 2020 18:00:46.854670048 CET	67.23.227.19	443	192.168.2.3	49737	CN=*.lamun.pk CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Oct 27 22:33:43 CET 2020 Thu Mar 17 17:40:46 CET 2016	Mon Jan 25 22:33:43 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 13, 2020 18:00:48.050462008 CET	192.254.225.195	443	192.168.2.3	49738	CN=cpanel.rcclabbd.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Nov 13 11:07:04 CET 2020	Thu Feb 11 11:07:04 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Dec 13, 2020 18:01:01.329282999 CET	192.3.183.226	443	192.168.2.3	49747	CN=webmail.thecype.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Oct 17 20:11:48 CEST 2020	Fri Jan 15 19:11:48 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5312 Parent PID: 5628

General

Start time:	17:59:56
Start date:	13/12/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\v1Us5AICBm.dll'
Imagebase:	0x13d0000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 6160 Parent PID: 5312

General

Start time:	18:00:40
Start date:	13/12/2020
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe
Imagebase:	0x1140000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Xyd	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ana	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Rasun	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Moox	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Ypt	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Agfo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Awan	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Emur	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Iwu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Yrku	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Nit	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ommim	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ibi	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Ywfoe	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3651F2	CreateDirectoryW
C:\Users\user\AppData\Roaming\Xyd\yvek.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	369651	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36BC62	HttpSendRequestA

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Xyd\yvek.dll	unknown	389120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 88 8d 3d 42 cc ec 53 11 cc ec 53 11 cc ec 53 11 5b 28 2d 11 cd ec 53 11 eb 2a 3e 11 c3 ec 53 11 eb 2a 2e 11 de ec 53 11 eb 2a 28 11 ca ec 53 11 eb 2a 3d 11 cb ec 53 11 0f e3 0e 11 c9 ec 53 11 cc ec 52 11 2b ec 53 11 eb 2a 21 11 94 ec 53 11 eb 2a 29 11 cd ec 53 11 eb 2a 2f 11 cd ec 53 11 eb 2a 2b 11 cd ec 53 11 52 69 63 68 cc ec 53 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.........=B..S...S...S.[(-... S..*>...S..*....S..*(...S..*=. ..S.......S...R.+.S..*!...S..*)...S..*/...S..*+...S.Rich..S.	success or wait	1	369680	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\v1Us5AICBm.dll	unknown	389120	success or wait	1	35A6C2	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Tyfe	success or wait	1	352290	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\brya	success or wait	1	363DD7	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\brya	ilyo	binary	42 AC AA 2C 0E 53 59 8A 8C E1 35 12 A3 3C 7C 8D 4A 1F 61 0E E7 99 95 31 14 FF D2 E8 2B 68 EB E1 FB 8F 7F CE 08 D0 01 EA 48 AD 95 9E DB D7 4A 30 2C F1 AD 19 CD 35 C8 5B 4E A7 F4 5E B2 47 CD 62 C0 C6 E5 1E E9 DA 50 70 9C 6C C7 0D D7 34 B0 25 23 3D 74 D6 AD 06 A7 D5 C4 F5 2E E3 1E 54 2E 03 26 DB 6D 1C 4C FC 60 14 97 95 9F 43 92 54 2F F0 C0 6F 6F 97 CF CB 0A 5D AB EC 89 B5 4A 1E 4E 73 74 C7 0E 6A AF 93 22 6B 56 77 70 16 74 2D 00 0D 17 E8 B8 8D C5 1C 24 67 F2 F6 39 59 4A EC 58 AD C4 4A 98 D0 F1 C8 E3 EE F9 24 AB CA 2F 65 CD 31 10 13 ED 74 15 89 FE F1 DF FF FE DC 86 78 55 35 04 E5 04 5D 9C 8D E0 BE 78 EC B0 47 D9 A0 29 CC 57 4E F8 E7 81 CC B2 CC 21 86 7A 32 DF 48 30 D9 A1 06 2E 33 C6 1B CE A9 D8 26 C0 DC 84 BC F2 E1 A8 77 4F 7D 58 55 8B 35 CF D0 D6 E3 83 09 DE 0B 40 C4 40 6F 07 ED 08 00	success or wait	1	363E1A	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			66 9A 4C E8 1D 74 C1 EB CB 29 6A B6 05 98 AF 6E 14 9B C2 4A 3E F1 5E D8 0B 97 FE 27 3C 66 03 16 04 57 F2 A6 17 8B CD 06 A1 EF 7C 49 62 AD EA F5 5A 4B 08 0E 5B 15 4C 8C B3 8D 4E A0 1A A0 43 05 DD 0E 3F CA 48 9D 27 E6 CD 85 D1 71 27 92 BD A0 68 D0 61 2E B6 3B D3 B9 36 1C FA D3 14 F8 77 33 7E F9 99 AB 9A 4D B3 A7 2E 96 D9 94 96 91 DA 26 0F 1E 08 CF 41 17 53 9A 1D FF 77 8A F1 67 F3 14 53 C1 19 53 69 30 D8 37 AA 8E 95 53 13 65 15 62 1E 15 B2 AC 7A A4 FF F1 F3 B8 0B 39 BD B6 3B A5 C9 4A 49 C5 C0 F6 87 22 E1 6C C0 F9 F7 C5 B2 D4 C2 23 E5 4F 6B 9A D9 17 C3 AF 0D 3B 61 96 6B 86 C3 2F B9 B5 DC 28 AD FC 78 11 E6 79 26 1D 34 CB 87 8C 8D 31 BA A2 AB 46 83 26 BE AA 6D 69 8D 35 A8 0C 06 AE A8 A9 F5 01 70 C2 B2 67 AA FC 50 40 91 87 A9 95 84 84 0D D0 2D 3A 9B CB 37 4D 31 4A 27 F9 4D D3 BC 8C 6B 45 C7 9E 17 17 E8 72 74 AF 35 1D 13 7C F4 D8 C4 47 B7 10 15 0A F6 74 ED CF 56 67 F6 39 0C 69 7A D3 CE 39 6B D9 DE DB E6 30 A4 FA EE 99 3B 3E 6A AB B0 EE D3 23 5C 5C BD C0 2C 80 B6 4E C8 18 15 9D 58 97 F8 BC D3 37 73 31 51 41 E0 16 C3 3A DB FE A3 AA 8E 14 CA 32 68 7D 11 D5 67 12 28 88 8C 95 A0 08 BD 1A DD 8E BC 96 DC A7 EE FB 77 E4 14 53 5F A4 64 12 99 90 EB 8B 01 E2 B6 42 96 09 BA 16 F0 78 68 A7 04 96 4C 0E A8 E8 03 E9 29 FB B0 4A 7B 4F 44 70 FB 75 03 8A 0F F9 A8 36 16 42 B0 B9 84 87 24 D8 B7 D2 97 CC D7 36 3A CD 2A 61 88 B0 2D 05 45 72 0D B0 D9 C5 85 00 01 21 77 95 FC 90 E9 76 CB DA 16 24 A0 8E EA BE 09 FE F7 5A 87 25 2C 78 35 3F 9F 5E EA F8 FF DA 04 3C 0F 14 88 16 58 52 03 27 F9 C5 7B 9D 62 F3 44 1A 2F 37 A3 03 A3 D7 6F E4 43 E9 5F B4 7A 8C B8 C1 6B 4B E5 CE 3A D5 51 C5 CB ED 4A D0 E6 D2 83 9A 22 DD 51 F1 1F 89 42 2D 85 C1 15 98 3B 4A 60 95 4F BF 72 E9 53 B5 28 B3 9A A9 97 DD 94 37 16 1D 27 FD B6 38 4E FC 0D D8 D7 71 41 C4 08 1D 7E 65 8B 48 9C 9B 58 64 1F 9B 82 68 D5 3E 5D 8C 01 86 30 96 79 7D 5F 16 E4 C6 2A 91 AD FC 7B 5C 7B 40 04 51 13 4A 5E 91 CE 7B FE CD 71 78 49 49 E9 88 20 45 2F 3F 2C 65 A9 81 8A A4 47 45 42 4A 17 38 70 9C 5C CE 52 6A 3B D2 E4 26 7B 1F D6 EC F7 A7 4D 5F F3 CC 32 0D 25 46 8A 37 8F 7E 58 25 F3 AE 0C EE 67 9E DE 0C 1D 66 18 7D 5E BF FC C3 6E E4 2C 10 3B 54 97 BB 71 BF B0 71 3A CE 13 A8 DE F9 6F 16 5D E4 98 70 98 68 2F 3C 96 D6 05 5A 5B 98 48 BA 3A CD D3 5C 84 7E 36 85 80 D8 76 D9 C9 8D A2 B6 F3 F6 3F 39 2F F7 30 98 0F C8 D0 16 9D EF 55 D9 24 96 E5 7A 90 60 66 14 0F 41 F1 65 73 6B 8D 4B 1E 24 1C 62 CB B6 13 6D 8B F5 9E 1C EC 14 AD B1 D3 4F 03 2A 88 4C 2F 01 70 8B 9F 7B 8D 9F E0 CF 47 D9 8D 4D 39 CA 5A 7E F6 1F BD 5A 10 FC 3A CF AC EC 13 D2 50 9B 87 CA 2D FC E6 76 ED 83 C1 2F 32 6D 10 16 C8 D6 FD 05 E4 2F 1C 9B 94 0F FD 15 9C 25 19 35 25 0E A8 52 3C DC 2B 6E FD 46 59 19 2B 88 4E 41 1F 82 4E 48 00 45 6F C2 71 FA A4 DC AC 23 11 D4 5C 79 18 87 3F 16 C8 AB 09 25 6D 84 6D 15 21 F1 62 C3 89 7D AA 7C 30 E2 A0 6E 98 EC 72 33 A2 14 1D 43 32 CD 08 B5 A4 EF 4B 04 41 BC 39 5E 3C 26 3E AE FE 8E BB 8C 8D F7 BB 43 05 97 81 BA FD 97 56 C7 8A				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Tyfe	gybuebad	binary	B0 EF 1D A4 66 6F 78 6F DC AB C4 74 5C 09 74 12 11 5C 7B CF E2 C0 9C A6 EF F8 30 F5 7D E5 6A 61 E8 5D D6 43 58 1A 4F 11 01 79 6E DA 8E 4F 22 9B F7 98 10 33 75 79 2A 41 5C 5D 93 FE 8B 88 16 D0 D4 1E 2A AD A6 EE 77 51 28 1C BC B8 7B 09 BA 4F 9D 98 10 7D C3 89 41 C2 3E 48 72 64 9A B7 EB 95 58 DE 8C 08 E4 37 97 9A 7E 6B D9 A1 6D CC 6E 61 F0 58 EC 62 A8 19 E3 66 85 DD 40 F6 9F 6E B7 C8 B5 68 33 D0 2C C6 61 80 EF 25 45 25 CF E5 E5 9E C3 E1 E6 E8 A9 92 A8 AD B8 6F 2F 9F 0D 83 18 59 A6 2F B9 0C AC 84 AF 02 BF CC A8 18 56 B9 07 89 22 6F 73 C9 48 89 2C 13 78 CF 83 DE D7 7A 15 33 80 68 CA 45 B5 B2 D2 48 2C A8 07 53 AA AE E8 A8 A6 A0 69 28 69 5D 6D D0 6C 3C A0 2C 25 0A 87 EC 6E 05 2B A7 FB E1 62 01 11 26 0D 4D 1A CF 94 55 88 E1 79 F7 5D 3C 5F 31 3D F9 7A C0 32 73 5E A5 32 1C 54 89 EF 30 3C 29 1A 50 A1 24 CC 84 28 83 2B 30 C0 93	success or wait	1	363E1A	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Tyfe	gybuebad	binary	B0 EF 1D A4 66 6F 78 6F DC AB C4 74 5C 09 74 12 11 5C 7B CF E2 C0 9C A6 EF F8 30 F5 7D E5 6A 61 E8 5D D6 43 58 1A 4F 11 01 79 6E DA 8E 4F 22 9B F7 98 10 33 75 79 2A 41 5C 5D 93 FE 8B 88 16 D0 D4 1E 2A AD A6 EE 77 51 28 1C BC B8 7B 09 BA 4F 9D 98 10 7D C3 89 41 C2 3E 48 72 64 9A B7 EB 95 58 DE 8C 08 E4 37 97 9A 7E 6B D9 A1 6D CC 6E 61 F0 58 EC 62 A8 19 E3 66 85 DD 40 F6 9F 6E B7 C8 B5 68 33 D0 2C C6 61 80 EF 25 45 25 CF E5 E5 9E C3 E1 E6 E8 A9 92 A8 AD B8 6F 2F 9F 0D 83 18 59 A6 2F B9 0C AC 84 AF 02 BF CC A8 18 56 B9 07 89 22 6F 73 C9 48 89 2C 13 78 CF 83 DE D7 7A 15 33 80 68 CA 45 B5 B2 D2 48 2C A8 07 53 AA AE E8 A8 A6 A0 69 28 69 5D 6D D0 6C 3C A0 2C 25 0A 87 EC 6E 05 2B A7 FB E1 62 01 11 26 0D 4D 1A CF 94 55 88 E1 79 F7 5D 3C 5F 31 3D F9 7A C0 32 73 5E A5 32 1C 54 89 EF 30 3C 29 1A 50 A1 24 CC 84 28 83 2B 30 C0 93	5E 90 2B F3 82 7F A5 17 D6 BE AC C9 CE B6 1B F6 B9 88 E1 FF E7 C5 99 A3 EA FD 35 F0 7B E3 6C 67 D4 98 0C F8 04 25 31 BD 12 A6 5B 0C 05 E2 F8 C1 AD C2 4A 69 2F 23 70 1B 06 07 C9 A4 D1 D2 4C 8A 8E 44 70 F7 FC B4 2D 0B 72 46 E6 E2 21 53 E0 15 2E 48 E4 97 55 1D 9B C1 AE C9 2C 93 9D EF C8 D7 B8 E5 C0 7A 62 B9 E7 39 FF F1 D9 E6 96 05 C4 DF 31 B8 6B 8F 1D 8E 02 88 6D CE F0 69 38 8C 9D 0A 73 46 CA BE 6C A9 F5 20 6B AD EA FB 19 63 E7 D6 FC B8 52 57 4F 9B ED 14 9F AB 9F A3 8E 24 47 21 40 D9 9D 5F 69 0B 91 DD D5 00 50 E9 12 ED 1A 9A 20 4F 71 CA E4 9A 97 DA 96 14 BE D7 58 66 DD B3 19 2D 32 13 F7 9B 6C C4 C6 D0 A3 63 68 8B C5 EC C5 EC 1A 34 8C E5 B1 EC 99 0E B1 07 30 DD D7 87 26 A9 5C C0 86 85 AB 9B 94 5A 12 C4 4C 1D 94 8F B3 53 CF C9 B9 9A 78 61 E2 96 C2 7D 9A 4F A7 14 B0 31 98 86 87 85 BD 2B 74 BC 34 F3 27 15 D0 0B 30 2B 35 B1 2E 89 90 3C D6 D0 9C 54 B6 1A 61 3C BF 76 9D 1F 91 97 B9 15 62 1A 5C 8B 57 7A C7 A2 C9 8B 6F FA 91 3D 58	success or wait	1	363E1A	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Tyfe	gybuebad	binary	5E 90 2B F3 82 7F A5 17 D6 BE AC C9 CE B6 1B F6 B9 88 E1 FF E7 C5 99 A3 EA FD 35 F0 7B E3 6C 67 D4 98 0C F8 04 25 31 BD 12 A6 5B 0C 05 E2 F8 C1 AD C2 4A 69 2F 23 70 1B 06 07 C9 A4 D1 D2 4C 8A 8E 44 70 F7 FC B4 2D 0B 72 46 E6 E2 21 53 E0 15 2E 48 E4 97 55 1D 9B C1 AE C9 2C 93 9D EF C8 D7 B8 E5 C0 7A 62 B9 E7 39 FF F1 D9 E6 96 05 C4 DF 31 B8 6B 8F 1D 8E 02 88 6D CE F0 69 38 8C 9D 0A 73 46 CA BE 6C A9 F5 20 6B AD EA FB 19 63 E7 D6 FC B8 52 57 4F 9B ED 14 9F AB 9F A3 8E 24 47 21 40 D9 9D 5F 69 0B 91 DD D5 00 50 E9 12 ED 1A 9A 20 4F 71 CA E4 9A 97 DA 96 14 BE D7 58 66 DD B3 19 2D 32 13 F7 9B 6C C4 C6 D0 A3 63 68 8B C5 EC C5 EC 1A 34 8C E5 B1 EC 99 0E B1 07 30 DD D7 87 26 A9 5C C0 86 85 AB 9B 94 5A 12 C4 4C 1D 94 8F B3 53 CF C9 B9 9A 78 61 E2 96 C2 7D 9A 4F A7 14 B0 31 98 86 87 85 BD 2B 74 BC 34 F3 27 15 D0 0B 30 2B 35 B1 2E 89 90 3C D6 D0 9C 54 B6 1A 61 3C BF 76 9D 1F 91 97 B9 15 62 1A 5C 8B 57 7A C7 A2 C9 8B 6F FA 91 3D 58	B7 D3 95 7A 81 6D F7 97 9D AC F1 F5 D3 DC 82 FE BC A8 54 50 55 77 2B 11 58 4F 87 42 C8 50 DF D4 CE 6B 1F A2 30 3E D5 05 2A 91 EE 4F E4 D8 61 41 2D 42 CA E9 AF A3 F0 9B 86 87 49 24 51 52 CC 0A 0E C4 F0 77 7C 34 AD 8B F2 C6 66 62 A1 D3 60 95 AE C8 64 17 D5 9D 1B 41 2E 49 AC 13 1D 6F 48 57 38 65 40 FA E2 83 F2 12 89 88 9C 53 BE 7E B1 A0 B3 8F 84 29 A1 4C F9 74 4C 6E 8D 98 07 4B 2E A2 6E CF D1 7E 1C DA C4 32 2C 84 28 DE 99 1E EF F8 F1 E7 5F DC D2 1E D8 62 58 99 48 F7 4A 86 F5 51 1B 41 52 47 B1 80 66 4E C1 9C C5 3A D7 F4 3A 28 E8 01 95 EE 74 83	success or wait	1	363E1A	RegSetValueExW

Disassembly

Code Analysis