ID: 404149
Sample Name: iJdlvBxhYu.dll
Cookbook: default.jbs
Time: 18:51:40
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report iJdlvBxhYu.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
Private 9
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 17
Sections 17

Resources 17
Imports 17
Exports 17
Version Infos 18
Possible Origin 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 19
TCP Packets 20
UDP Packets 21
DNS Queries 22
DNS Answers 22
HTTP Request Dependency Graph 23
HTTP Packets 24
Code Manipulations 24
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: loaddll32.exe PID: 6684 Parent PID: 5920 24
General 25
File Activities 25
Analysis Process: cmd.exe PID: 6692 Parent PID: 6684 25
General 25
File Activities 25
Analysis Process: rundll32.exe PID: 6720 Parent PID: 6684 25
General 25
File Activities 25
Analysis Process: rundll32.exe PID: 6732 Parent PID: 6692 26
General 26
File Activities 26
Analysis Process: rundll32.exe PID: 6780 Parent PID: 6684 26
General 26
File Activities 27
Analysis Process: iexplore.exe PID: 6728 Parent PID: 792 27
General 27
File Activities 27
Registry Activities 27
Analysis Process: iexplore.exe PID: 4876 Parent PID: 6728 27
General 27
File Activities 27
Disassembly 28
Code Analysis 28

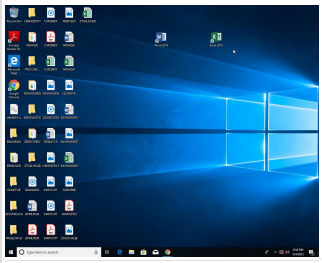
Analysis Report iJdlvBxhYu.dll

Overview

General Information

Sample Name:	iJdlvBxhYu.dll
Analysis ID:	404149
MD5:	18d613d02eaf8d3.
SHA1:	01ea39853139cc..
SHA256:	bd43f7bc23a76b0.
Tags:	dll geo Gozi ISFB ITA Ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

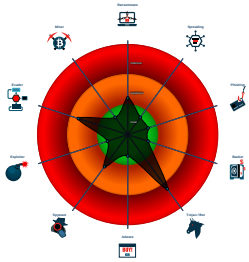
Ursnif

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Contains functionality which may be…
- Creates a process in suspended mo…
- Detected potential crypto function
- Found potential string decryption / a…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6684 cmdline: loaddll32.exe 'C:\Users\user\Desktop\iJdlvBxhYu.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6692 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\iJdlvBxhYu.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6732 cmdline: rundll32.exe 'C:\Users\user\Desktop\iJdlvBxhYu.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6720 cmdline: rundll32.exe C:\Users\user\Desktop\iJdlvBxhYu.dll,Enterbeen MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6780 cmdline: rundll32.exe C:\Users\user\Desktop\iJdlvBxhYu.dll,Multiply MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6728 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4876 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6728 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"KfAh1HjBYV5+GLf1H4+++WQcflLYE80sojTEX/uvXaLXhDxSfFOCIe7aHw1TYNxXIBvEkznlAveWMvLVTSjkgy/Hqpm47GUbXiPUxbpl0qoDhGQpz45mxRQlc+jgXQ4D03Y0gMF90NeOpBOEi497zfDlURi8Me7OHCSUNpn4Q0kQtrInhQlll9V6IFuYjZJB",
  "c2_domain": [
    "outlook.com/login",
    "gmail.com",
    "dorelunonu.us",
    "morelunonu.us"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```

Yara Overview

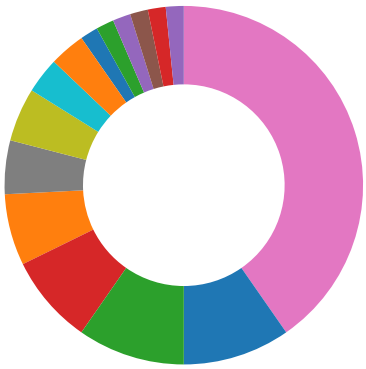
Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.536297010.0000000005618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.536331315.0000000005618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.536410675.0000000005618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.536390845.0000000005618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.536247273.0000000005618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

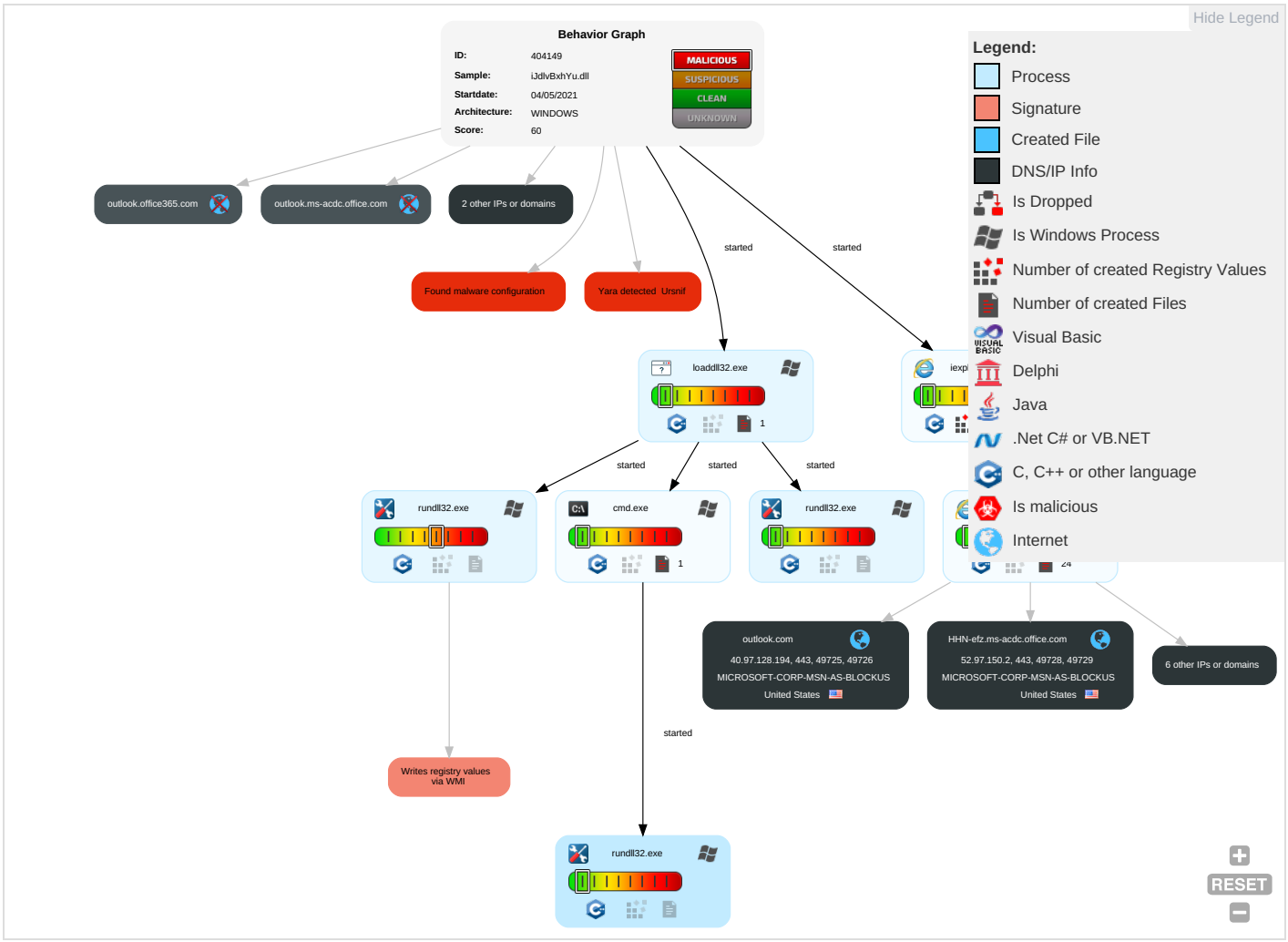
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

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
iJdlvBxhYu.dll	6%	Virustotal		Browse
iJdlvBxhYu.dll	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.1000000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
outlook.com	40.97.128.194	true	false		high
HHN-efz.ms-acdc.office.com	52.97.150.2	true	false		high
FRA-efz.ms-acdc.office.com	52.97.201.82	true	false		high
www.outlook.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high

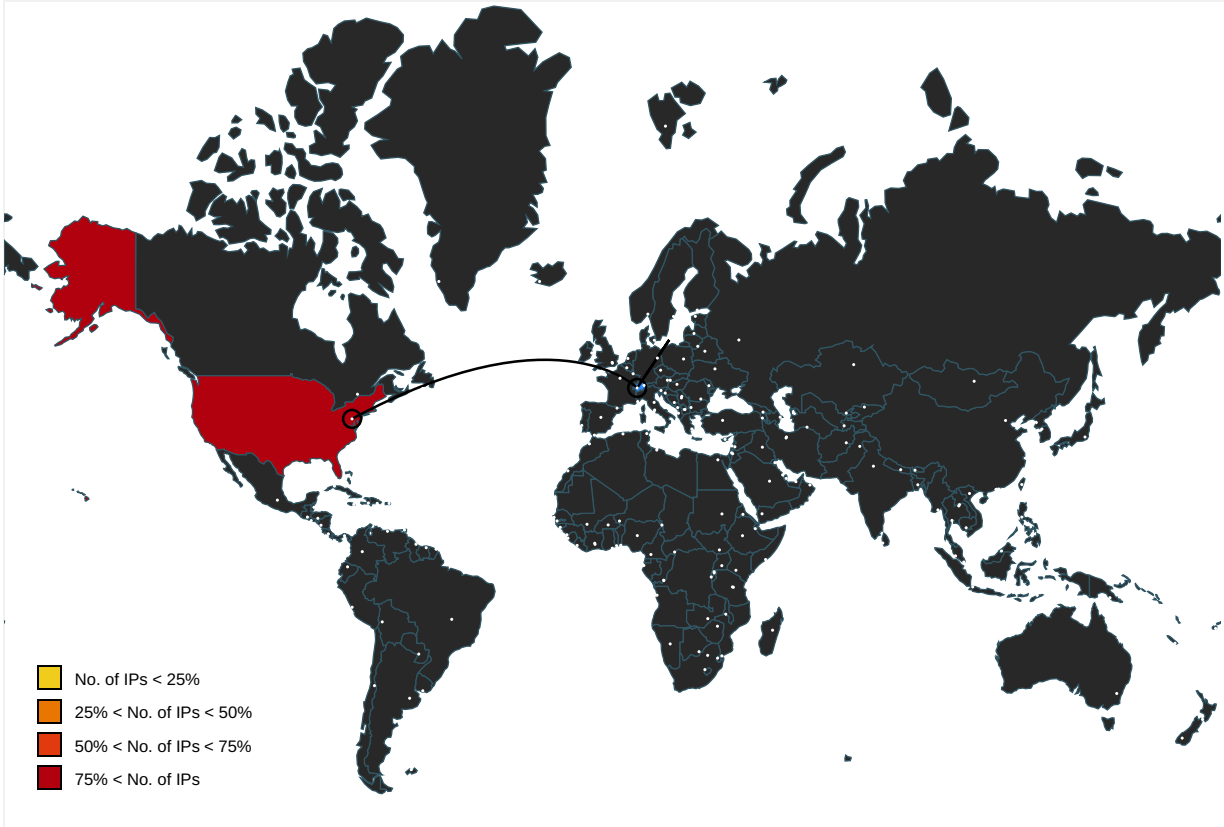
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://outlook.com/login/greed/dTdjBCYANBp89r_2BxCJb/gK6KRSDvLFl65FiM/sVGCJkg_2FiGctf/t6MCq4h_2BQjlakLCK/wiH0Ze_2B/jucB0Ra6kWTVhbib9MO1/jbq6SBoLka4DWlxdGWZ/y4sF0OuALvDiDjUoj2_2B_/2FCnNAucowWTY/QocXWkvP/dNKrsXhuwJ0UrXUCqZRpNCx/r6rZ7E04g_/2B8ZRdIhu4yR4YZKp/tqA3A0JYvM/21FVchV.gfk	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/login/greed/dTdjBCYANBp89r_2BxCJb/gK6KRSDvLFl65FiM/sVGCJkg_2FiGctf/t6M	~DF0D80EB75D4D79339.TMP.15.dr, {C4CF6A29-AD44-11EB-90E5-ECF4BB2D2496}.dat.15.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.97.150.2	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.97.128.194	outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.201.82	FRA-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404149
Start date:	04.05.2021
Start time:	18:51:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	iJdlvBxhYu.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:	22
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:	mal60.troj.winDLL@12/5@3/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.2% (good quality ratio 8.7%) • Quality average: 79.3% • Quality standard deviation: 28.8%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 92.122.145.220, 52.147.198.201, 104.43.193.48, 8.238.27.126, 8.238.28.254, 8.241.79.126, 8.238.29.254, 8.241.88.254, 2.20.142.209, 2.20.142.210, 20.190.160.132, 20.190.160.6, 20.190.160.67, 20.190.160.71, 20.190.160.136, 20.190.160.4, 20.190.160.8, 20.190.160.73, 20.82.210.154, 92.122.213.247, 92.122.213.194, 184.30.24.56, 88.221.62.148, 152.199.19.161, 40.64.100.89, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, mw1eap.displaycatalog.md.mp.microsoft.com.akadns.net, fg.download.windowsupdate.com.c.footprint.net, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, consumerrp-displaycatalog-aks2eap-uswest.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, displaycatalog-uswesteap.md.mp.microsoft.com.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:53:49	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.97.150.2	SCAN08364720 #45836(PDF).pdf.htm	Get hash	malicious	Browse	
40.97.128.194	http://outlook.com/owa/airmasteraustralia.onmicrosoft.com	Get hash	malicious	Browse	• outlook.com/owa/airmasteraustralia.onmicrosoft.com
52.97.201.82	DHL Notification -AWB DHL-2021011293002.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HHN-efz.ms-acdc.office.com	8OKQ6ogGRx.dll	Get hash	malicious	Browse	• 40.101.138.2
	609110f2d14a6.dll	Get hash	malicious	Browse	• 40.101.137.34
	New%20order%20contract.html	Get hash	malicious	Browse	• 52.98.175.2
outlook.com	n6osajjc938.exe	Get hash	malicious	Browse	• 104.47.54.36
	9b3d7f02.exe	Get hash	malicious	Browse	• 104.47.54.36
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 52.101.24.0
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 104.47.53.36
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 52.101.24.0
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 104.47.53.36
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 104.47.54.36
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 104.47.54.36
	SecuriteInfo.com.W32.AIDetect.malware2.29567.exe	Get hash	malicious	Browse	• 104.47.53.36
	lsass(1).exe	Get hash	malicious	Browse	• 104.47.59.138
	rtofwqxq.exe	Get hash	malicious	Browse	• 104.47.53.36
	VufxYArno1.exe	Get hash	malicious	Browse	• 104.47.53.36
FRA-efz.ms-acdc.office.com	8OKQ6ogGRx.dll	Get hash	malicious	Browse	• 40.101.81.162
	dechert-Investment078867-xlsx.Html	Get hash	malicious	Browse	• 52.97.189.66
	murexltd-Investment_265386-xlsx.html	Get hash	malicious	Browse	• 52.97.188.66
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 52.97.250.226
	sgs-Investment974041-xlsx.Html	Get hash	malicious	Browse	• 40.101.19.162
	roccor-invoice-648133_xls.HtMl	Get hash	malicious	Browse	• 52.97.200.162
	redwirespace-invoice-982323_xls.HtMl	Get hash	malicious	Browse	• 40.101.12.82
	prismcosec-invoice-647718_xls.HtMl	Get hash	malicious	Browse	• 40.101.81.130
	E848.tmp.exe	Get hash	malicious	Browse	• 40.101.81.130
	Payment.html	Get hash	malicious	Browse	• 52.97.250.194
	Remittance advice.htm	Get hash	malicious	Browse	• 52.97.250.210
	0G2gue8shl.exe	Get hash	malicious	Browse	• 52.97.176.2
	February Payroll.xls.htm	Get hash	malicious	Browse	• 52.97.250.242
	PURCHASE ORDER#34556558.exe	Get hash	malicious	Browse	• 52.97.200.178
	Proforma Invoice.exe	Get hash	malicious	Browse	• 52.97.250.210
	E-DEKONT.exe	Get hash	malicious	Browse	• 52.97.144.178
	DHL Notification -AWB DHL-2021011293002.exe	Get hash	malicious	Browse	• 52.97.201.82
	DHL DOCS.exe	Get hash	malicious	Browse	• 40.101.80.2
	ORDER REQUEST.exe	Get hash	malicious	Browse	• 40.101.121.34
	INVOICE.exe	Get hash	malicious	Browse	• 52.97.188.66

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	2f50000.exe	Get hash	malicious	Browse	• 52.141.33.89
	609110f2d14a6.dll	Get hash	malicious	Browse	• 40.101.137.34
	EBqJhAymeE.rtf	Get hash	malicious	Browse	• 157.55.173.72
	QXfU5ZSUpd.exe	Get hash	malicious	Browse	• 20.194.35.6
	813oo3jeWE.exe	Get hash	malicious	Browse	• 20.184.2.45
	pog.exe	Get hash	malicious	Browse	• 40.124.7.222
	8UsA.sh	Get hash	malicious	Browse	• 20.233.3.158
	pog.exe	Get hash	malicious	Browse	• 40.124.7.222
	nT7K5GG5km	Get hash	malicious	Browse	• 40.96.198.202
	KnAY2OIPI3	Get hash	malicious	Browse	• 20.177.182.208
	krJF4BtzSv.exe	Get hash	malicious	Browse	• 65.52.188.118
	DSOneApp(1).exe	Get hash	malicious	Browse	• 40.126.31.141
	INV 57474545.doc	Get hash	malicious	Browse	• 65.52.188.118
	kr.ps1	Get hash	malicious	Browse	• 204.79.197.200
	JRyLnlTR1O	Get hash	malicious	Browse	• 20.176.121.146

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New%20order%20contract.html	Get hash	malicious	Browse	• 52.98.175.2
	ldr.sh	Get hash	malicious	Browse	• 20.3.143.189
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• 65.52.188.118
	confirm this order and sign PI.exe	Get hash	malicious	Browse	• 13.66.245.231
	CMEpJtxLhf.exe	Get hash	malicious	Browse	• 52.168.94.29
MICROSOFT-CORP-MSN-AS-BLOCKUS	2f50000.exe	Get hash	malicious	Browse	• 52.141.33.89
	609110f2d14a6.dll	Get hash	malicious	Browse	• 40.101.137.34
	EBqJhAymeE.rtf	Get hash	malicious	Browse	• 157.55.173.72
	QXfU5ZSUpd.exe	Get hash	malicious	Browse	• 20.194.35.6
	813oo3jeWE.exe	Get hash	malicious	Browse	• 20.184.2.45
	pog.exe	Get hash	malicious	Browse	• 40.124.7.222
	8UsA.sh	Get hash	malicious	Browse	• 20.233.3.158
	pog.exe	Get hash	malicious	Browse	• 40.124.7.222
	nT7K5GG5km	Get hash	malicious	Browse	• 40.96.198.202
	KnAY2OIPI3	Get hash	malicious	Browse	• 20.177.182.208
	krJF4BtzSv.exe	Get hash	malicious	Browse	• 65.52.188.118
	DSOneApp(1).exe	Get hash	malicious	Browse	• 40.126.31.141
	INV 57474545.doc	Get hash	malicious	Browse	• 65.52.188.118
	kr.ps1	Get hash	malicious	Browse	• 204.79.197.200
	JRyLnlTR1O	Get hash	malicious	Browse	• 20.176.121.146
	New%20order%20contract.html	Get hash	malicious	Browse	• 52.98.175.2
	ldr.sh	Get hash	malicious	Browse	• 20.3.143.189
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• 65.52.188.118
	confirm this order and sign PI.exe	Get hash	malicious	Browse	• 13.66.245.231
	CMEpJtxLhf.exe	Get hash	malicious	Browse	• 52.168.94.29

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{C4CF6A27-AD44-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7690028446621529
Encrypted:	false
SSDEEP:	48:IwOGcprWGwpL3G/ap8vZGIpcKGYGvnZpvKcGomRqp9KXGo4qW1pmEjGWmzy1MGWu:rSZOZ/2vLWbt6AfPqW1MfODIL+TNRDB
MD5:	7002C28F8DAFB19C321D8F3802742CAC
SHA1:	10586DB11264F5FB282E742B7C439209155B4A41
SHA-256:	AF3751488A7F551AE1A019B306EC610845E7424749F28AE6BF40C9F8BDFEC153
SHA-512:	74ABC47BE2FA0394B397E0BCC83052452EC870C0141D01FF9CCAC3A284C556DD7464D9692CABAC3A64A7B015B5C5EC0A5153F528752C65ABC0D3F463CEF1DDB
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C4CF6A29-AD44-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27440
Entropy (8bit):	1.8692767005485296

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C4CF6A29-AD44-11EB-90E5-ECF4BB2D2496}.dat	
Encrypted:	false
SSDEEP:	192:r+ZdQF6fkZj52dWxMN64GBKG7x4GBKGuA:rKiwcVI0Kguouq
MD5:	8FA8A2AC554320BF7B927691D0E9AA33
SHA1:	37BB604AF62C4236281E0640728FAB1A40E61068
SHA-256:	5CFA609F2EE9DD30D833ADF282288AB25CBE0619EF014B63A2D71DD0636FD61E
SHA-512:	DC3570C168CC2174D16E1908AAFB7C3C4BDD8E13192131EAFA8FB6F91D7E4717CFF5B49FC9B29F6E41D77A18388A53EFD7668760024C4603851EECE09719690
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.440534734931472
Encrypted:	false
SSDEEP:	3:oVXUWRFEfQRcS4T48JOGXnEWRFEfQRcS4uULun:o9UChcwqEChcS7
MD5:	5B1B55767347E99D9DF8CFDEA6ABE92F
SHA1:	21E2F35CA929750943C12141583CCA5D3EAB76A3
SHA-256:	A93DEB522A49F2709E978A2F8F1B8A35FBF8B9EAFA8AF6499EC096BE71E0555A
SHA-512:	B4FE7A36552EE0BF60DB9781C17B8A7F2E8B81D6C67B1480319C26C1E6B8D898AAC7C23374414E59594A65E67E4404BCBBDEE0EB22D9929EE6BD833EA1DBF5 70
Malicious:	false
Reputation:	low
Preview:	[2021/05/04 18:54:05.717] Latest deploy version: ..[2021/05/04 18:54:05.717] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF0D80EB75D4D79339.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39777
Entropy (8bit):	0.6001466555757741
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+CkuH0S4GBKGz4GBKG/4GBKGE:kBqoxKAuqR+CkuH0SuWueuX
MD5:	648119EC3976EFE617D1F81C477C1B69
SHA1:	941D0AD9905FF41F28A51FC7463C7E80E63DFBAC
SHA-256:	0AE66953DBE3EBBC42F7D50BFF3568F07E10D28C9205B89CBCADFA5FD327A0D4
SHA-512:	3DD2AEF4769544D679FE1BCDF7D18408AE61C5070D1123914D46CC4AED5890D0F217B31AC77990A554A2ED7CE49D694030A85F17B9223D62516C97E765186ED
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF222070F69DD5E09D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4101257122829776
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lof9lof9lWJatrFat5B:kBqoIAeo10fB
MD5:	0182845E86B74629EC312B38783F6A31
SHA1:	B0FBDA728E7F1458FF95368C850A0CC9F5C534B8
SHA-256:	73172B66EC5FE590A7CC6F5F2CC197082ABCC57AF15A2943A739F91995081D4F
SHA-512:	8FD0EEE8E84724EC60A73A512D834F87297AD6A40260A25C4EF97BD0CFE513B690B177164E351D32AAD994E1A12D211486826BCC5038CA629E4C65AED74745C
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF222070F69DD5E09D.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.549323607622641
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:	iJdlvBxhYu.dll
File size:	523264
MD5:	18d613d02eaf8d339feebb21f578f329
SHA1:	01ea39853139ccfe82f0bd19f8963d3ccebf8e8a
SHA256:	bd43f7bc23a76b086a81b8e6fcd4355cac648d3f7d9a941d9aa259def534d5b1
SHA512:	a432ca4267f56530945e2dd352e658d72b3fc84101b84dcd86bc0adcf42e218e394556d6b69cec92cb30a960ce83586e8c026e971f02fa5154d100a198f1e4ce
SSDEEP:	12288:CddaT8lLVrp6I7MsfHqWxSWlNTjGoLYTbgOJpXLH:Cddhp1YCMuFx/jGo0XL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.G.....T.....AN.....V.....i.....h....^.B.....l.....U.....R.....W.....Rich.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x104a38a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6089CC25 [Wed Apr 28 20:57:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	61abfa6d76443dd7d018df0c9cf8b0a5

Entrypoint Preview

Instruction
push ebp
mov ebp, esp

Instruction
cmp dword ptr [ebp+0Ch], 01h
jne 00007FD0D4954B07h
call 00007FD0D495B0D4h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FD0D4954B0Ch
add esp, 0Ch
pop ebp
retn 000Ch
push 0000000Ch
push 0107B4A8h
call 00007FD0D4955A1Ch
xor eax, eax
inc eax
mov esi, dword ptr [ebp+0Ch]
test esi, esi
jne 00007FD0D4954B0Eh
cmp dword ptr [0118E36Ch], esi
je 00007FD0D4954BEAh
and dword ptr [ebp-04h], 00000000h
cmp esi, 01h
je 00007FD0D4954B07h
cmp esi, 02h
jne 00007FD0D4954B37h
mov ecx, dword ptr [01075238h]
test ecx, ecx
je 00007FD0D4954B0Eh
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call ecx
mov dword ptr [ebp-1Ch], eax
test eax, eax
je 00007FD0D4954BB7h
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call 00007FD0D4954916h
mov dword ptr [ebp-1Ch], eax
test eax, eax
je 00007FD0D4954BA0h
mov ebx, dword ptr [ebp+10h]
push ebx
push esi
push dword ptr [ebp+08h]
call 00007FD0D4952376h
mov edi, eax
mov dword ptr [ebp-1Ch], edi
cmp esi, 01h
jne 00007FD0D4954B2Ah
test edi, edi
jne 00007FD0D4954B26h
push ebx
push eax
push dword ptr [ebp+08h]
call 00007FD0D495235Eh
push ebx
push edi
push dword ptr [ebp+08h]
call 00007FD0D49548DCh
mov eax, dword ptr [01075238h]
test eax, eax
je 00007FD0D4954B09h

Instruction
push ebx
push edi
push dword ptr [ebp+08h]
call eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x7bbd0	0x58	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7bc28	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x191000	0x498	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x192000	0x2818	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6b200	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x7a980	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x6b000	0x1ac	.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	0x6988d	0x69a00	False	0.70416512574	data	6.62140187581	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6b000	0x115e0	0x11600	False	0.471967738309	data	5.23669501131	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7d000	0x113300	0x1800	False	0.333984375	data	3.88700180982	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x191000	0x498	0x600	False	0.356119791667	data	2.99935790597	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x192000	0x2818	0x2a00	False	0.743117559524	data	6.59705049508	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1910a0	0x35c	data	English	United States
RT_MANIFEST	0x191400	0x91	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	FlushFileBuffers, GetConsoleCP, GetConsoleMode, SetEnvironmentVariableA, SetStdHandle, SetFilePointerEx, WriteConsoleW, CloseHandle, GetFileAttributesW, GetWindowsDirectoryW, CreateProcessW, OpenMutexW, VirtualProtectEx, EncodePointer, DecodePointer, HeapAlloc, GetSystemTimeAsFileTime, RaiseException, RtlUnwind, GetCommandLineA, GetCurrentThreadId, IsProcessorFeaturePresent, GetLastError, HeapFree, ExitProcess, GetModuleHandleExW, GetProcAddress, AreFileApisANSI, MultiByteToWideChar, WideCharToMultiByte, HeapSize, GetStdHandle, WriteFile, GetModuleFileNameW, GetProcessHeap, IsDebuggerPresent, GetTimeZoneInformation, SetLastError, GetCurrentThread, GetFileType, DeleteCriticalSection, GetStartupInfoW, GetModuleFileNameA, QueryPerformanceCounter, GetCurrentProcessId, GetEnvironmentStringsW, FreeEnvironmentStringsW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, InitializeCriticalSectionAndSpinCount, CreateEventW, Sleep, GetCurrentProcess, TerminateProcess, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetTickCount, GetModuleHandleW, CreateSemaphoreW, SetConsoleCtrlHandler, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, EnterCriticalSection, LeaveCriticalSection, FatalAppExitA, FreeLibrary, LoadLibraryExW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, HeapReAlloc, OutputDebugStringW, GetStringTypeW, CreateFileW
USER32.dll	GetPropW, CreateMenu, DeferWindowPos, BeginDeferWindowPos, UnregisterHotKey, TranslateMessage, RegisterWindowMessageW
GDI32.dll	MoveToEx, SetTextColor, SetBkMode, SetBkColor, LineTo, IntersectClipRect, GetClipBox, GetCharWidthW, CreateBitmap
COMCTL32.dll	ImageList_SetDragCursorImage, ImageList_Draw, PropertySheetW, CreatePropertySheetPageA

Exports

Name	Ordinal	Address
Enterbeen	1	0x1047ed0
Multiply	2	0x1047fb0

Version Infos

Description	Data
LegalCopyright	Fingergeneral Corporation. All rights reserved
InternalName	Probable
FileVersion	5.5.2.216 Sidedone
CompanyName	Fingergeneral Corporation
ProductName	Fingergeneral Wear twenty
ProductVersion	5.5.2.216
FileDescription	Fingergeneral Wear twenty
OriginalFilename	turn.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Snort IDS Alerts

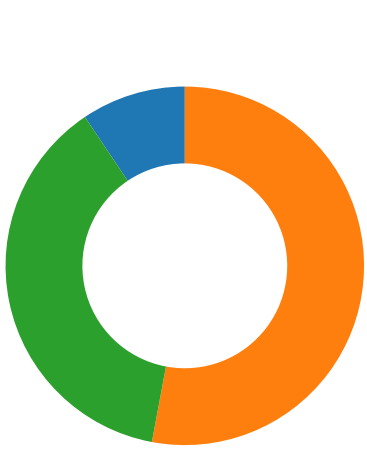
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-18:52:29.692083	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:29.727060	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/04/21-18:52:29.727454	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:29.763162	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
05/04/21-18:52:29.763557	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:29.799375	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.49.165	192.168.2.6
05/04/21-18:52:29.800094	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:29.840838	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.18	192.168.2.6
05/04/21-18:52:29.841596	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:29.888178	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.53	192.168.2.6
05/04/21-18:52:29.888557	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:29.935589	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.56.190	192.168.2.6
05/04/21-18:52:29.936007	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:29.981493	ICMP	449	ICMP Time-To-Live Exceeded in Transit			4.68.37.93	192.168.2.6
05/04/21-18:52:29.981978	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:33.661732	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:37.677969	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:41.678428	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-18:52:46.273239	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:50.163683	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:54.183288	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:52:58.210718	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:02.180671	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:06.166018	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:10.165814	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:14.165998	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:18.170708	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:22.187264	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:26.185740	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:30.169625	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:34.182432	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:38.621192	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:42.637472	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:46.627649	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:50.623633	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:54.618741	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:53:59.048851	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:02.619742	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:06.619825	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:10.620244	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:14.620372	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:18.627035	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:22.627997	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:26.622060	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:30.622421	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:34.623800	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:38.622781	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126
05/04/21-18:54:42.626771	ICMP	384	ICMP PING			192.168.2.6	8.238.27.126

Network Port Distribution

Total Packets: 85

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:54:06.545804977 CEST	49725	80	192.168.2.6	40.97.128.194
May 4, 2021 18:54:06.545804024 CEST	49726	80	192.168.2.6	40.97.128.194
May 4, 2021 18:54:06.689771891 CEST	80	49726	40.97.128.194	192.168.2.6
May 4, 2021 18:54:06.689989090 CEST	49726	80	192.168.2.6	40.97.128.194
May 4, 2021 18:54:06.690716028 CEST	49726	80	192.168.2.6	40.97.128.194
May 4, 2021 18:54:06.691628933 CEST	80	49725	40.97.128.194	192.168.2.6
May 4, 2021 18:54:06.691734076 CEST	49725	80	192.168.2.6	40.97.128.194
May 4, 2021 18:54:06.838143110 CEST	80	49726	40.97.128.194	192.168.2.6
May 4, 2021 18:54:06.838278055 CEST	49726	80	192.168.2.6	40.97.128.194
May 4, 2021 18:54:06.838489056 CEST	49726	80	192.168.2.6	40.97.128.194
May 4, 2021 18:54:06.846282005 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:06.982461929 CEST	80	49726	40.97.128.194	192.168.2.6
May 4, 2021 18:54:06.992594004 CEST	443	49727	40.97.128.194	192.168.2.6
May 4, 2021 18:54:06.992799997 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.001812935 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.150540113 CEST	443	49727	40.97.128.194	192.168.2.6
May 4, 2021 18:54:07.150578022 CEST	443	49727	40.97.128.194	192.168.2.6
May 4, 2021 18:54:07.150607109 CEST	443	49727	40.97.128.194	192.168.2.6
May 4, 2021 18:54:07.150631905 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.150660038 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.188564062 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.195911884 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.338144064 CEST	443	49727	40.97.128.194	192.168.2.6
May 4, 2021 18:54:07.338247061 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.346502066 CEST	443	49727	40.97.128.194	192.168.2.6
May 4, 2021 18:54:07.346637011 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.347060919 CEST	49727	443	192.168.2.6	40.97.128.194
May 4, 2021 18:54:07.414005995 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.414077997 CEST	49729	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.463756084 CEST	443	49729	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.463836908 CEST	443	49728	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.463890076 CEST	49729	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.463932991 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.464896917 CEST	49729	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.465254068 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.492871046 CEST	443	49727	40.97.128.194	192.168.2.6
May 4, 2021 18:54:07.514828920 CEST	443	49729	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.514866114 CEST	443	49729	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.514894009 CEST	443	49729	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.514909029 CEST	443	49728	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.514928102 CEST	443	49728	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.514945030 CEST	443	49728	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.515085936 CEST	49729	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.515105963 CEST	49728	443	192.168.2.6	52.97.150.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:54:07.515187025 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.525580883 CEST	49729	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.525724888 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.526541948 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.575365067 CEST	443	49728	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.575416088 CEST	443	49728	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.575449944 CEST	443	49729	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.575480938 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.575510979 CEST	49729	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.578187943 CEST	443	49728	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.578321934 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.578660965 CEST	49728	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:07.627228022 CEST	443	49728	52.97.150.2	192.168.2.6
May 4, 2021 18:54:07.639496088 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.639502048 CEST	49731	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.686299086 CEST	443	49730	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.686391115 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.687308073 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.692817926 CEST	443	49731	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.693005085 CEST	49731	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.703771114 CEST	49731	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.734812975 CEST	443	49730	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.734844923 CEST	443	49730	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.734864950 CEST	443	49730	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.735014915 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.745953083 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.746764898 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.757808924 CEST	443	49731	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.757838011 CEST	443	49731	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.757853985 CEST	443	49731	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.757935047 CEST	49731	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.758002996 CEST	49731	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.764975071 CEST	49731	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.793373108 CEST	443	49730	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.793854952 CEST	443	49730	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.793988943 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.799103975 CEST	443	49730	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.799125910 CEST	443	49730	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.799235106 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:07.819248915 CEST	443	49731	52.97.201.82	192.168.2.6
May 4, 2021 18:54:07.819401026 CEST	49731	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:08.096868038 CEST	443	49731	52.97.201.82	192.168.2.6
May 4, 2021 18:54:08.097042084 CEST	49731	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:08.861166954 CEST	49725	80	192.168.2.6	40.97.128.194
May 4, 2021 18:54:08.861208916 CEST	49730	443	192.168.2.6	52.97.201.82
May 4, 2021 18:54:08.861330986 CEST	49729	443	192.168.2.6	52.97.150.2
May 4, 2021 18:54:08.861331940 CEST	49731	443	192.168.2.6	52.97.201.82

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:52:22.970918894 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:23.019690037 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 18:52:23.403167009 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:23.463300943 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 18:52:24.167635918 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:24.216428041 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 18:52:24.945031881 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:24.996774912 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 18:52:26.020801067 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:26.069710016 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 18:52:27.312602997 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:27.361246109 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 18:52:28.160480022 CEST	56023	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:52:28.209218025 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 18:52:29.012883902 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:29.072856903 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 18:52:29.475900888 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:29.690892935 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 18:52:29.991524935 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:30.040215015 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 18:52:30.890821934 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 18:52:30.939558983 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 18:53:22.466109037 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 18:53:22.523046017 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 18:53:23.511240959 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 18:53:23.568932056 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 18:53:49.129221916 CEST	52811	53	192.168.2.6	8.8.8.8
May 4, 2021 18:53:49.194948912 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 18:53:49.752892971 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 18:53:49.804584980 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 18:53:52.110009909 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 18:53:52.170139074 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 18:54:02.225565910 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:02.287480116 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 18:54:05.205369949 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:05.264559984 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 18:54:06.474169970 CEST	50339	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:06.525335073 CEST	53	50339	8.8.8.8	192.168.2.6
May 4, 2021 18:54:07.356297970 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:07.405424118 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 18:54:07.588264942 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:07.637008905 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 18:54:25.366008043 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:25.414696932 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 18:54:32.429203033 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:33.435081959 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:33.497840881 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 18:54:35.170659065 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:35.219465971 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 18:54:36.184983969 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:36.233985901 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 18:54:37.201193094 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:37.249866962 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 18:54:39.216440916 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:39.265095949 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 18:54:40.336675882 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:40.486478090 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 18:54:41.825098038 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:42.024085999 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 18:54:42.507457018 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:42.566903114 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 18:54:43.000472069 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 18:54:43.051908016 CEST	53	62208	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 18:54:06.474169970 CEST	192.168.2.6	8.8.8.8	0xc384	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.356297970 CEST	192.168.2.6	8.8.8.8	0x97c4	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.588264942 CEST	192.168.2.6	8.8.8.8	0x3bca	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 18:53:49.194948912 CEST	8.8.8.8	192.168.2.6	0x7009	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:54:06.525335073 CEST	8.8.8.8	192.168.2.6	0xc384	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 4, 2021 18:54:06.525335073 CEST	8.8.8.8	192.168.2.6	0xc384	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 4, 2021 18:54:06.525335073 CEST	8.8.8.8	192.168.2.6	0xc384	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 4, 2021 18:54:06.525335073 CEST	8.8.8.8	192.168.2.6	0xc384	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 4, 2021 18:54:06.525335073 CEST	8.8.8.8	192.168.2.6	0xc384	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 4, 2021 18:54:06.525335073 CEST	8.8.8.8	192.168.2.6	0xc384	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 4, 2021 18:54:06.525335073 CEST	8.8.8.8	192.168.2.6	0xc384	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 4, 2021 18:54:06.525335073 CEST	8.8.8.8	192.168.2.6	0xc384	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.405424118 CEST	8.8.8.8	192.168.2.6	0x97c4	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:54:07.405424118 CEST	8.8.8.8	192.168.2.6	0x97c4	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:54:07.405424118 CEST	8.8.8.8	192.168.2.6	0x97c4	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:54:07.405424118 CEST	8.8.8.8	192.168.2.6	0x97c4	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:54:07.405424118 CEST	8.8.8.8	192.168.2.6	0x97c4	No error (0)	HHN-efz.ms-acdc.office.com		52.97.150.2	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.405424118 CEST	8.8.8.8	192.168.2.6	0x97c4	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.18	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.405424118 CEST	8.8.8.8	192.168.2.6	0x97c4	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.18	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.405424118 CEST	8.8.8.8	192.168.2.6	0x97c4	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.50	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.637008905 CEST	8.8.8.8	192.168.2.6	0x3bca	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:54:07.637008905 CEST	8.8.8.8	192.168.2.6	0x3bca	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:54:07.637008905 CEST	8.8.8.8	192.168.2.6	0x3bca	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 18:54:07.637008905 CEST	8.8.8.8	192.168.2.6	0x3bca	No error (0)	FRA-efz.ms-acdc.office.com		52.97.201.82	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.637008905 CEST	8.8.8.8	192.168.2.6	0x3bca	No error (0)	FRA-efz.ms-acdc.office.com		52.97.144.2	A (IP address)	IN (0x0001)
May 4, 2021 18:54:07.637008905 CEST	8.8.8.8	192.168.2.6	0x3bca	No error (0)	FRA-efz.ms-acdc.office.com		52.97.170.34	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- outlook.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49726	40.97.128.194	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:54:06.690716028 CEST	1192	OUT	GET /login/greed/dTdjBCYANBp89r_2BxCJb/gK6KRSDvLFl65FiM/sVGCJkg_2FiGctf/t6MCq4h_2BQjlakLCK/wiH0Ze_2B/jucB0Ra6kWTVhbib9MO1/jbq6SBoLka4DWlxdGWZ/y4sF0OuALvDiDjUoj2_2B_/2FCnNAucowWTY/QocXWkvP/dNKrsXhuwJ0UrXUCqZRpNCx/r6rZ7E04g_/2B8ZRdIhu4yR4YZKp/tqA3A0JYvM/21FVchV.gfk HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: outlook.com Connection: Keep-Alive
May 4, 2021 18:54:06.838143110 CEST	1192	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/login/greed/dTdjBCYANBp89r_2BxCJb/gK6KRSDvLFl65FiM/sVGCJkg_2FiGctf/t6MCq4h_2BQjlakLCK/wiH0Ze_2B/jucB0Ra6kWTVhbib9MO1/jbq6SBoLka4DWlxdGWZ/y4sF0OuALvDiDjUoj2_2B_/2FCnNAucowWTY/QocXWkvP/dNKrsXhuwJ0UrXUCqZRpNCx/r6rZ7E04g_/2B8ZRdIhu4yR4YZKp/tqA3A0JYvM/21FVchV.gfk Server: Microsoft-IIS/10.0 request-id: 8a3df280-21c9-49ae-91ea-af755b4bfa8a X-FEServer: DM5PR2201CA0020 X-RequestId: 90931448-0ba3-4c8d-8c41-ca4c654f378b X-Powered-By: ASP.NET X-FEServer: DM5PR2201CA0020 Date: Tue, 04 May 2021 16:54:06 GMT Connection: close Content-Length: 0

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: loaddll32.exe PID: 6684 Parent PID: 5920

General

Start time:	18:52:30
Start date:	04/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\iJdlvBxhYu.dll'
Imagebase:	0xa50000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6692 Parent PID: 6684

General

Start time:	18:52:30
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\iJdlvBxhYu.dll',#1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6720 Parent PID: 6684

General

Start time:	18:52:30
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\iJdlvBxhYu.dll,Enterbeen
Imagebase:	0x1040000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6732 Parent PID: 6692

General

Start time:	18:52:30
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\iJdlvBxhYu.dll',#1
Imagebase:	0x1040000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536297010.0000000005618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536331315.0000000005618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536410675.0000000005618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536390845.0000000005618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536247273.0000000005618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536484271.0000000005618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.595047356.0000000005618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536426256.0000000005618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.536360413.0000000005618000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6780 Parent PID: 6684

General

Start time:	18:52:33
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\iJdlvBxhYu.dll,Multiply
Imagebase:	0x1040000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6728 Parent PID: 792

General

Start time:	18:54:04
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	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

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: iexplore.exe PID: 4876 Parent PID: 6728

General

Start time:	18:54:04
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6728 CREDAT:17410 /prefetch:2
Imagebase:	0x40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	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

Disassembly

Code Analysis