ID: 410818
Sample Name: 609a460e94791.tiff.dll
Cookbook: default.jbs
Time: 11:09:21
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

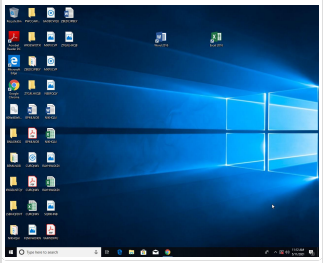
Analysis Report 609a460e94791.tiff.dll

Overview

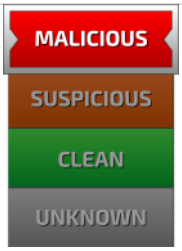
General Information

Sample Name:	609a460e94791.tiff.dll
Analysis ID:	410818
MD5:	50a299d1e92d92..
SHA1:	c188272ab757db..
SHA256:	3b56b7298c366a..
Tags:	BRT dll geo gozi isfb ita ursnif
Infos:	

Most interesting Screenshot:



Detection



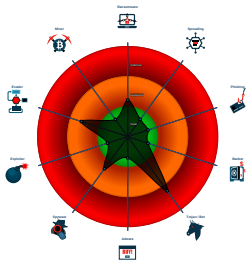
Ursnif

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- 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 read the PEB
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- Extensive use of GetProcAddress (o…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6660 cmdline: loaddll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6672 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6700 cmdline: rundll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6688 cmdline: rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Hundredpopulate@@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6736 cmdline: rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Mark@@12 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6760 cmdline: rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Seefit@@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5436 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5924 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5436 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"KujE77ctKyR8x3/dODwZbEsxGmck+FW9384s5u0Kacw8y1gCN+8m2bfjJPovkn+Uzufcdfss+a43eI6oHR1KgWQmvEAO6LK8tJv+Wl7iCBPJP7eef8xKeXht/Mhk1PSj7mHnJ9lcqKMtTteEdSecVvMRtb/WSKVTFfHDva9My7AJ/NbX
qHdzCG7znACswLxD",
  "c2_domain": [
    "outlook.com/login",
    "gmail.com",
    "worunekulo.club",
    "horunekulo.website"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```

Yara Overview

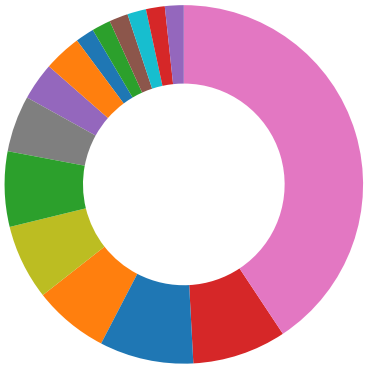
Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.662417377.0000000003EA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.681209868.0000000005148000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000002.724251151.0000000003EA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.662378098.0000000003EA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.662456772.0000000003EA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 15 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 or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

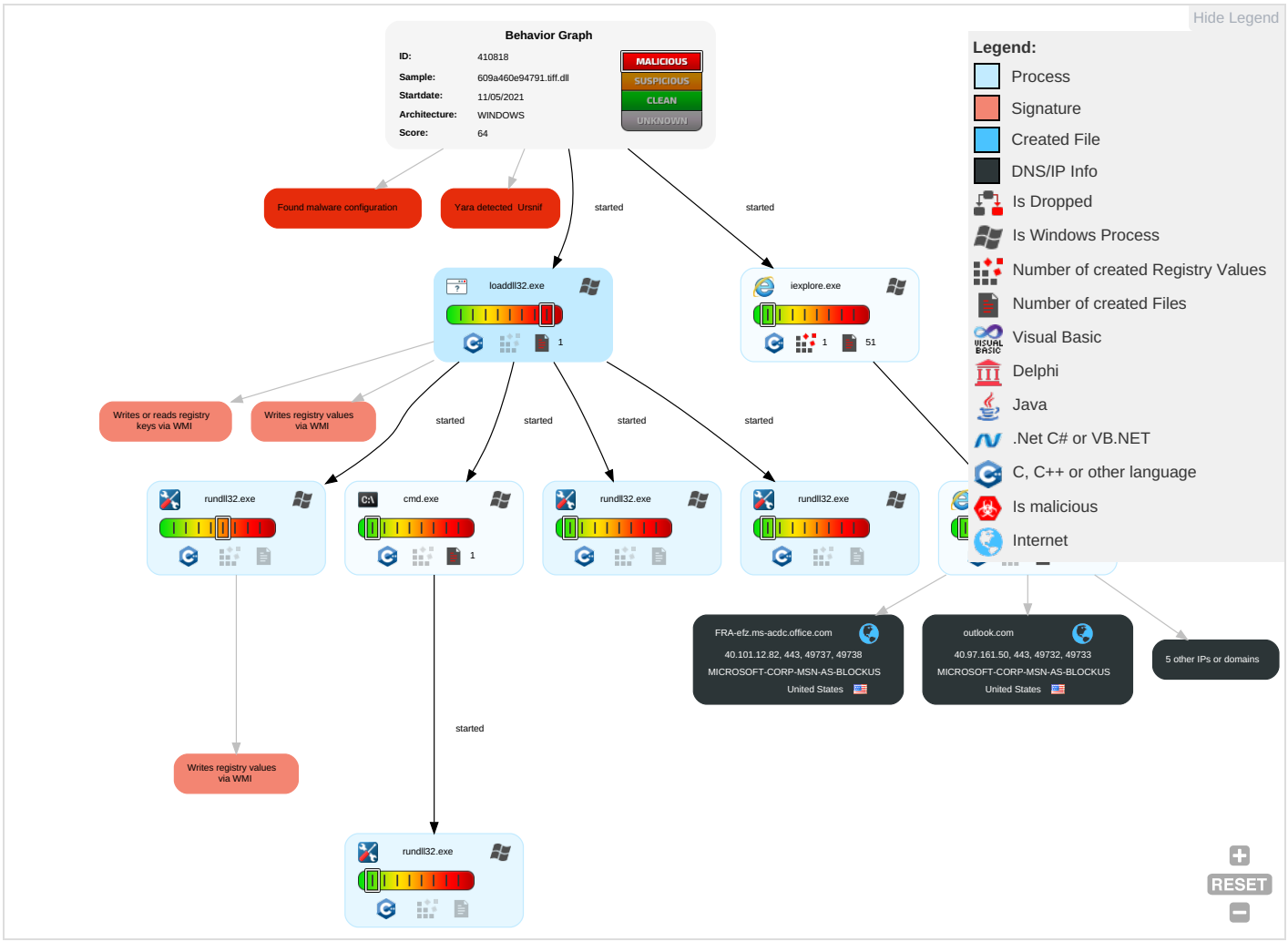
Remote Access Functionality:

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	Re Se Eff
Valid Accounts	Windows Management Instrumentation 2	Application Shimming 1	Process Injection 1 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Application Shimming 1	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Ob De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	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	Software Packing	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	Steganography	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 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

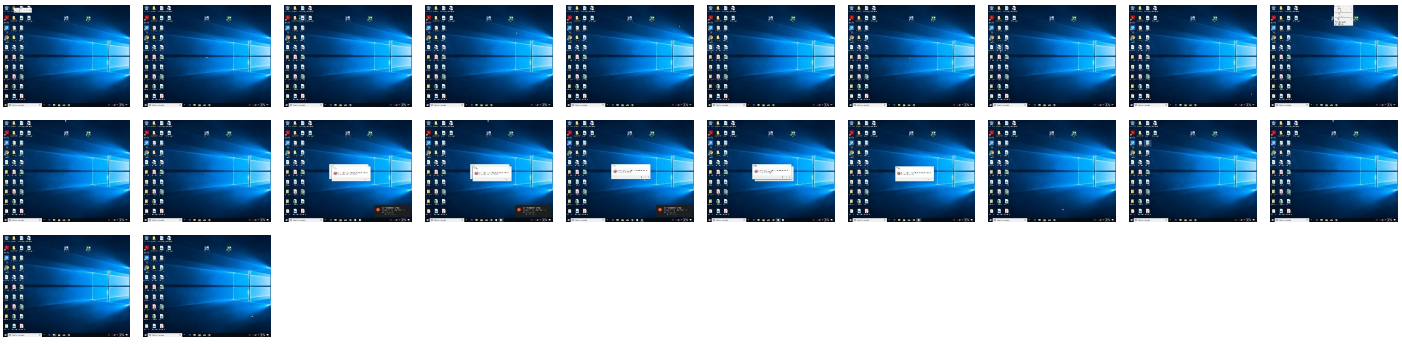
Behavior Graph



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
609a460e94791.tiff.dll	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.2c90000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.1620000.0.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	40.97.161.50	true	false		high
HHN-efz.ms-acdc.office.com	52.97.201.34	true	false		high
FRA-efz.ms-acdc.office.com	40.101.12.82	true	false		high
www.outlook.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high

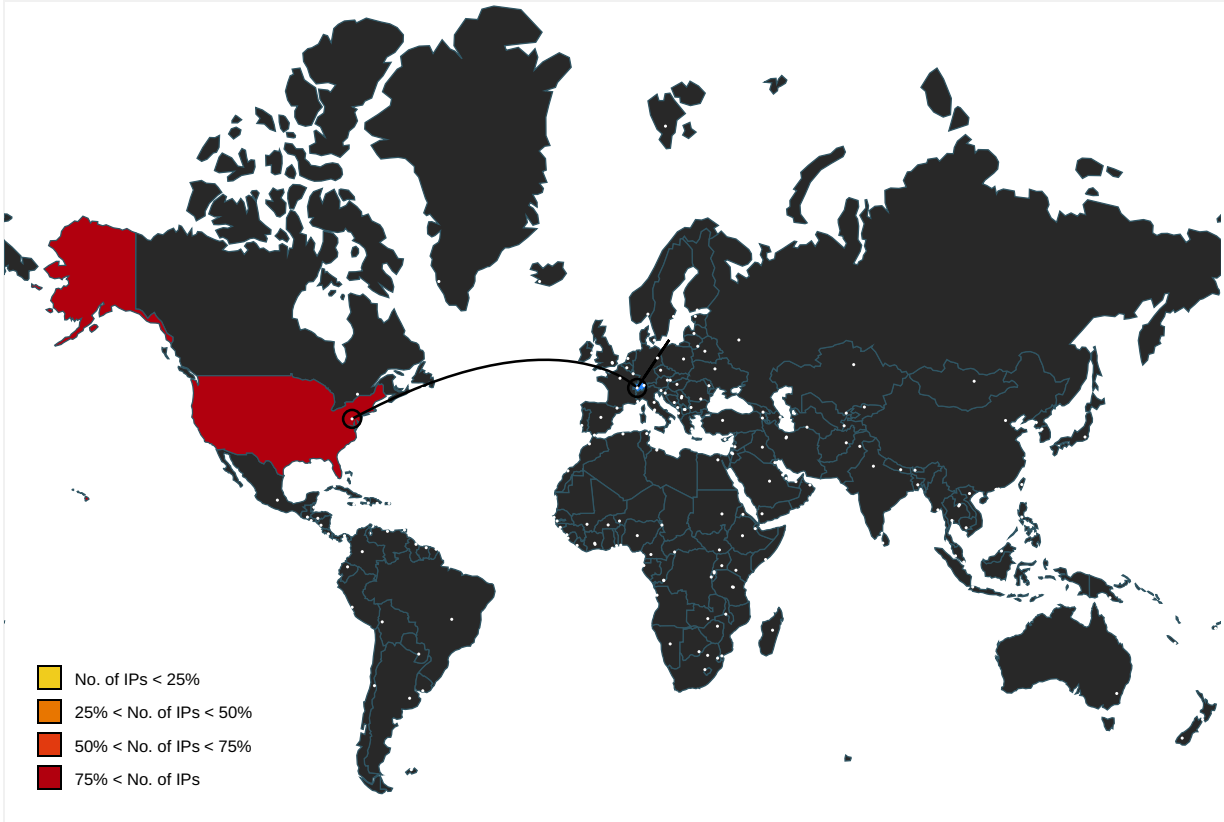
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://outlook.com/login/greed/gx9NI4Ybpp/8F85m84ndjn4UwJSZ/KFY_2BxmUPMy/coa0QUktAbb/vjBaicl7yvyNDs/NaAVAq9mPnbNTlKz1AUy2/5aIKWQiZNRBNaijS/Tt5Vo5dnaNIMeJI/Piqfb55cpfCEI8CpHK/_2FWICMIW/YUkQnOfGVld1SPd1rTnm/w0s_2F9NNcplFjkZ_2F/ufX9zF863VCJiOMFbmL1SV/K4t8NhPa8Lg/cl7PdmL.gfk	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/login/greed/gx9NI4Ybpp/8F85m84ndjn4UwJSZ/KFY_2BxmUPMy/coa0QUktAbb/vjBa	~DF6A2029352AAD8EB0.TMP.18.dr, {7A4756FC-B284-11EB-90E5-ECF4BB2D2496}.dat.18.dr	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	410818
Start date:	11.05.2021
Start time:	11:09:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	609a460e94791.tiff.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	29
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:	mal64.troj.winDLL@14/5@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.3% (good quality ratio 9.7%) • Quality average: 79.1% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 64% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 52.147.198.201, 92.122.145.220, 168.61.161.212, 52.255.188.83, 205.185.216.42, 205.185.216.10, 184.30.24.56, 13.64.90.137, 40.126.31.141, 20.190.159.136, 20.190.159.138, 40.126.31.4, 40.126.31.143, 40.126.31.139, 40.126.31.1, 40.126.31.137, 20.50.102.62, 13.88.21.125, 92.122.213.194, 92.122.213.247, 88.221.62.148, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.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, au.download.windowsupdate.com.hwcdn.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, 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, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, cds.d2s7q6s2.hwcdn.net, www.tm.a.prd.aadg.akadns.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.97.201.34	New%20order%20contract.html	Get hash	malicious	Browse	
40.97.161.50	13fil.exe	Get hash	malicious	Browse	
	24messag.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	66documen.exe	Get hash	malicious	Browse	
	9messag.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
40.101.12.82	redwirespace-invoice-982323_xls.HtMl	Get hash	malicious	Browse	
	http://https://user74359648.ts.r.appspot.com/#jodymontgomery@technologyunderstood.com	Get hash	malicious	Browse	
	https:\\bit.ly/3bulbTy#eric.tuliao@ibo.org	Get hash	malicious	Browse	
	http://https://iau-maskan.ir	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
outlook.com	file.msg.exe	Get hash	malicious	Browse	• 104.47.56.138
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 104.47.57.138
	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
HHN-efz.ms-acdc.office.com	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.150.2
	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
FRA-efz.ms-acdc.office.com	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.201.82
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	ilOO9qC8yj.exe	Get hash	malicious	Browse	• 13.107.4.50
	qLi9sAxeSm.exe	Get hash	malicious	Browse	• 204.95.99.243
	f1a5fbd3e946e8db1c18bd1d30d0f8b41a873cbb76769.exe	Get hash	malicious	Browse	• 20.194.35.6
	tgix.exe	Get hash	malicious	Browse	• 137.117.64.85
	Protiviti.htm	Get hash	malicious	Browse	• 52.240.156.143
	hn80vhR3y1.exe	Get hash	malicious	Browse	• 13.69.222.243
	file.msg.exe	Get hash	malicious	Browse	• 104.47.56.161
	SCB_MT103_31951R2105050031_200505.PDF.exe	Get hash	malicious	Browse	• 157.55.136.23
	Windows_Update.exe	Get hash	malicious	Browse	• 20.52.178.148
	NcLDA3J4Kp.apk	Get hash	malicious	Browse	• 204.79.197.200
	Llau1wwvy5.exe	Get hash	malicious	Browse	• 20.43.33.61
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 104.47.37.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.201.82
	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
MICROSOFT-CORP-MSN-AS-BLOCKUS	iIoO9qC8yj.exe	Get hash	malicious	Browse	• 13.107.4.50
	qLi9sAxeSm.exe	Get hash	malicious	Browse	• 204.95.99.243
	f1a5fbd3e946e8db1c18bd1d30d0f8b41a873cbb76769.exe	Get hash	malicious	Browse	• 20.194.35.6
	tgix.exe	Get hash	malicious	Browse	• 137.117.64.85
	Protiviti.htm	Get hash	malicious	Browse	• 52.240.156.143
	hn80vhR3y1.exe	Get hash	malicious	Browse	• 13.69.222.243
	file.msg.exe	Get hash	malicious	Browse	• 104.47.56.161
	SCB_MT103_31951R2105050031_200505.PDF.exe	Get hash	malicious	Browse	• 157.55.136.23
	Windows_Update.exe	Get hash	malicious	Browse	• 20.52.178.148
	NcLDA3J4Kp.apk	Get hash	malicious	Browse	• 204.79.197.200
	LIau1wwvy5.exe	Get hash	malicious	Browse	• 20.43.33.61
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 104.47.37.36
	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.201.82
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7A4756FA-B284-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.767330112336001
Encrypted:	false
SSDEEP:	48:IwhGcprYGwpLdjG/ap8nGIpcFmQGvnZpvFkaGocnRqp9F0jGo4gnsn1pm6GWcnzA:rXZAZdD2ZWkJtGAfBeS1Mj6GICKT/NDB
MD5:	156D3CAF9E8A794ADFC20BEF63EEA127
SHA1:	AF7F7711A0A50AC466904AF1088B915D447CC937
SHA-256:	52D1E225E5A48663A4E782CEE505EF4EFCB03B57D86EB1AEAE2BCB514D55FA88
SHA-512:	E5F0BF27719A6BE7C63C2D1976443B37CCE0741EE08096BF7757B7501CDE2EF28B2183CB5DEB5A34B514D5EFD36D40EAD7F4599EAC060613ED12F05C928833 2
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\{7A4756FC-B284-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7A4756FC-B284-11EB-90E5-ECF4BB2D2496}.dat	
Category:	dropped
Size (bytes):	27428
Entropy (8bit):	1.864673958093044
Encrypted:	false
SSDEEP:	96:rrZYQ06AHBSYjB/2RWBkMyG2NXLER2NXLnA:rrZYQ06AHkYjB/2RWBkMyG2NbER2NbnA
MD5:	AD45202875B5B3222E4A0FA70E557E36
SHA1:	262462EB28F2EE5AA4AB87168782A3225D7C2766
SHA-256:	322B18772F6CEE64ACF8D3DF9A5B5E189FC5C11ED8113396D3E8A080C6F73F57
SHA-512:	8B4786EDCC10EB81485BB689D2FEAADBECDC52E7DA026E7D6201D77D84D86C5CC368F844FAB8B1AA7E95B7418599A11E63719EFD1F3772E6594F99C69C8C7 48
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):	4.21211232961955
Encrypted:	false
SSDEEP:	3:oVXUXhXf7Tz8JOGXnEXhXf7T4LX+n:o9UXhP7vqEXhP7Su
MD5:	D37E17C754DC8265F6B19F375B3B2A7B
SHA1:	DB6EB0959B70CB613479E0C56B4B298F120A12C5
SHA-256:	98D3B53E62F7515A00599868EC0299B37D4A3F09B2C864023EC62A52CE8A8356
SHA-512:	B0AE75F39E8D1EFB9ED6136F128166053A01E3FE9A971DA55993FBEE36ECCF09D8747E912C1D98D69634454ECD93E29A7546F8ADE9D1B5157052009359C882C
Malicious:	false
Reputation:	low
Preview:	[2021/05/11 11:12:44.310] Latest deploy version: ..[2021/05/11 11:12:44.310] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF6A2029352AAD8EB0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39753
Entropy (8bit):	0.5952183110788842
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+lLpY7t2NXLY2NXLk2NXLd:kBqoxKAuqR+lLpY7t2NbY2Nbk2Nbd
MD5:	3332CE02133F1A2B17659763DD9F9ED8
SHA1:	2CCFF0E9B9AC268A48483F244C2549AC30046A95
SHA-256:	9EB41D80206763DADE5A30133DF5EDEBA27E69BAFDFA96FC9C438933A7B93518
SHA-512:	06AD119BF6B0ECF2397AED8527A4BD69057E52365B10129408DFB61DC62C6D8B7CEC88EC54E360CFADC7BAEB785B5652FD27C0F255AEEDD056D66FC5B1C77 B7
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF745550B0ECD73E02.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4106988703667074
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo19loV9lWGOyqyN4:kBqoI+glt9
MD5:	B7796152E2D67FE2A933DE459C627111
SHA1:	ADDA7FFAC9F85AAF9ADD7FFED33C359333CF2017
SHA-256:	8FE8BAB0CBA61FF6244059D467FE8A550F96650FA9B247DA1C5C99F64C68AC2E

C:\Users\user\AppData\Local\Temp\~DF745550B0ECD73E02.TMP

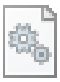
SHA-512:	CB66D870F71B7BCB93B74276733079062BCDD216183D64C5624235C797887BFEA7DCAAB002A0ED2B644C118636B7B45C279B0CB7F0ADA8338DC2FE724DCD67 E
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	6.388590209681191
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Win16/32 Executable Delphi generic (2074/23) 0.21% • 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:	609a460e94791.tiff.dll
File size:	841216
MD5:	50a299d1e92d9205e123404c8e05904d
SHA1:	c188272ab757dbbf14e74781fc90fcefe4aeb615
SHA256:	3b56b7298c366a323d28658a455abf0d4e78fa197a43ce1 3bedab05f26901d34
SHA512:	ec30f36d70ddbb6ba4aaccb3342e0a0ffbd586d27843705 00a94e33aa650d1c56d3712ffc3a9e15a0558194ce26d1b 76d9f2a8953220684bef634e57f4579df1
SSDEEP:	12288:mzCoYRvNZrA8Res/TPUOjUUGcqcoWEx9kMG US6vOV5y4gnuD5wtqqB7ol:VdNZr5RLL1AZ/clUnHvk5 hgU
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L...L ..`...........!.................0.. @..........................{..x..

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1033080
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:	0x6092C34C [Wed May 5 16:09:48 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

General

Import Hash:	dc55991f7b8a912c780d10d352635290

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FC658BC9A27h
call 00007FC658BCA6F7h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call 00007FC658BC9806h
add esp, 0Ch
pop ebp
retn 000Ch
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov dword ptr [ebp-04h], ecx
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+08h]
mov ecx, dword ptr [eax]
mov dword ptr [ebp-04h], ecx
mov eax, dword ptr [ebp-04h]
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FC658BC99F9h
add esp, 04h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FC658BC9A99h
add esp, 04h
test eax, eax
je 00007FC658BC9A23h
int3
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FC658BC9A79h
add esp, 04h
test eax, eax
je 00007FC658BC9A29h
mov ecx, 00000041h
int 29h
pop ebp
ret
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx

Instruction
mov eax, dword ptr [ebp+08h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xc7bb0	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc7c28	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe8000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe9000	0x51e0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc5ecc	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xc5f20	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9b000	0x1a4	.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	0x997af	0x99800	False	0.488934942488	data	6.50079371898	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9b000	0x2d5aa	0x2d600	False	0.326892863292	data	4.74980452387	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc9000	0x1efdc	0xe00	False	0.209821428571	data	3.01039741419	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe8000	0x3a0	0x400	False	0.404296875	data	3.03375733203	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe9000	0x51e0	0x5200	False	0.770293445122	data	6.74990882481	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe8060	0x340	data	English	United States

Imports

DLL	Import
KERNEL32.dll	CreateFileW, GetWindowsDirectoryW, ReadFile, GetConsoleMode, OpenMutexW, CloseHandle, GetFileSize, DeleteCriticalSection, ReadConsoleW, VirtualProtectEx, GetConsoleCP, FlushFileBuffers, SetFilePointerEx, GetFileSizeEx, SetStdHandle, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, SetLastError, InitializeCriticalSectionAndSpinCount, CreateEventW, SwitchToThread, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetSystemTimeAsFileTime, GetTickCount, GetModuleHandleW, GetProcAddress, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, GetCurrentProcess, TerminateProcess, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, InitializeSListHead, RaiseException, RtlUnwind, InterlockedPushEntrySList, InterlockedFlushSList, GetLastError, EncodePointer, FreeLibrary, LoadLibraryExW, GetModuleFileNameW, GetModuleHandleExW, ExitProcess, HeapAlloc, HeapValidate, GetSystemInfo, GetCurrentThread, GetStdHandle, GetFileType, WriteFile, OutputDebugStringW, WriteConsoleW, SetConsoleCtrlHandler, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, GetProcessHeap, HeapFree, HeapReAlloc, HeapSize, HeapQueryInformation, DecodePointer
UxTheme.dll	CloseThemeData
AVIFIL32.dll	AVIFileGetStream, AVIFileOpenW, AVIFileExit, AVIFileInit, AVIFileEndRecord
TAPI32.dll	lineRedirectW, lineInitialize, lineHold, lineShutdown, lineTranslateAddressW

Exports

Name	Ordinal	Address
Hundredpopulate@@8	1	0x1030208
Mark@@12	2	0x10303fe
Seefit@@8	3	0x103046c

Version Infos

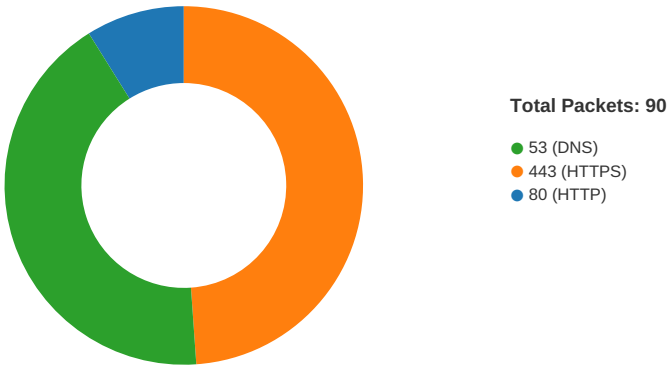
Description	Data
LegalCopyright	Dad plan Corporation. All rights reserved
InternalName	Team Lonesell
FileVersion	7.2.6.201
CompanyName	Dad plan Corporation
These	95
ProductName	Dad plan Fair fell
ProductVersion	7.2.6.201
FileDescription	Dad plan Fair fell
OriginalFilename	fall.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:12:44.427018881 CEST	49732	80	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.427045107 CEST	49733	80	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.607211113 CEST	80	49732	40.97.161.50	192.168.2.6
May 11, 2021 11:12:44.607337952 CEST	49732	80	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.608804941 CEST	49732	80	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.612221003 CEST	80	49733	40.97.161.50	192.168.2.6
May 11, 2021 11:12:44.612348080 CEST	49733	80	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.792617083 CEST	80	49732	40.97.161.50	192.168.2.6
May 11, 2021 11:12:44.792712927 CEST	49732	80	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.792838097 CEST	49732	80	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.806026936 CEST	49734	443	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.971962929 CEST	80	49732	40.97.161.50	192.168.2.6
May 11, 2021 11:12:44.987812042 CEST	443	49734	40.97.161.50	192.168.2.6
May 11, 2021 11:12:44.987920046 CEST	49734	443	192.168.2.6	40.97.161.50
May 11, 2021 11:12:44.997282028 CEST	49734	443	192.168.2.6	40.97.161.50

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:12:45.180705070 CEST	443	49734	40.97.161.50	192.168.2.6
May 11, 2021 11:12:45.180744886 CEST	443	49734	40.97.161.50	192.168.2.6
May 11, 2021 11:12:45.180768013 CEST	443	49734	40.97.161.50	192.168.2.6
May 11, 2021 11:12:45.180855989 CEST	49734	443	192.168.2.6	40.97.161.50
May 11, 2021 11:12:45.276611090 CEST	49734	443	192.168.2.6	40.97.161.50
May 11, 2021 11:12:45.285624981 CEST	49734	443	192.168.2.6	40.97.161.50
May 11, 2021 11:12:45.459654093 CEST	443	49734	40.97.161.50	192.168.2.6
May 11, 2021 11:12:45.460292101 CEST	49734	443	192.168.2.6	40.97.161.50
May 11, 2021 11:12:45.470313072 CEST	443	49734	40.97.161.50	192.168.2.6
May 11, 2021 11:12:45.472281933 CEST	49734	443	192.168.2.6	40.97.161.50
May 11, 2021 11:12:45.576265097 CEST	49734	443	192.168.2.6	40.97.161.50
May 11, 2021 11:12:45.659774065 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.661045074 CEST	49736	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.708501101 CEST	443	49735	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.709875107 CEST	443	49736	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.710011959 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.710911989 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.710912943 CEST	49736	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.711765051 CEST	49736	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.757880926 CEST	443	49734	40.97.161.50	192.168.2.6
May 11, 2021 11:12:45.760519028 CEST	443	49735	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.760541916 CEST	443	49735	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.760556936 CEST	443	49735	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.760607958 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.760670900 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.761409998 CEST	443	49736	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.761429071 CEST	443	49736	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.761445045 CEST	443	49736	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.761499882 CEST	49736	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.761563063 CEST	49736	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.774986029 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.776258945 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.784162045 CEST	49736	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.826571941 CEST	443	49735	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.827660084 CEST	443	49735	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.827770948 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.835220098 CEST	443	49735	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.835249901 CEST	443	49736	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.835447073 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.835484028 CEST	49736	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.835897923 CEST	49735	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:45.886379957 CEST	443	49735	52.97.201.34	192.168.2.6
May 11, 2021 11:12:45.918647051 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:45.922597885 CEST	49738	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:45.965564966 CEST	443	49737	40.101.12.82	192.168.2.6
May 11, 2021 11:12:45.965801001 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:45.966717958 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:45.974643946 CEST	443	49738	40.101.12.82	192.168.2.6
May 11, 2021 11:12:45.974823952 CEST	49738	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:45.975717068 CEST	49738	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.017079115 CEST	443	49737	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.017102003 CEST	443	49737	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.017115116 CEST	443	49737	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.017225027 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.031157017 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.031497955 CEST	443	49738	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.031522036 CEST	443	49738	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.031536102 CEST	443	49738	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.031650066 CEST	49738	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.031689882 CEST	49738	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.032501936 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.039944887 CEST	49738	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.079329014 CEST	443	49737	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.079353094 CEST	443	49737	40.101.12.82	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:12:46.079552889 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.085823059 CEST	443	49737	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.085839987 CEST	443	49737	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.085958958 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:46.094058990 CEST	443	49738	40.101.12.82	192.168.2.6
May 11, 2021 11:12:46.094203949 CEST	49738	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:48.734452009 CEST	49737	443	192.168.2.6	40.101.12.82
May 11, 2021 11:12:48.734502077 CEST	49733	80	192.168.2.6	40.97.161.50
May 11, 2021 11:12:48.734641075 CEST	49736	443	192.168.2.6	52.97.201.34
May 11, 2021 11:12:48.734688997 CEST	49738	443	192.168.2.6	40.101.12.82

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:10:04.627749920 CEST	62044	53	192.168.2.6	8.8.8.8
May 11, 2021 11:10:04.688019037 CEST	53	62044	8.8.8.8	192.168.2.6
May 11, 2021 11:10:05.065530062 CEST	63791	53	192.168.2.6	8.8.8.8
May 11, 2021 11:10:05.119048119 CEST	53	63791	8.8.8.8	192.168.2.6
May 11, 2021 11:10:05.514097929 CEST	64267	53	192.168.2.6	8.8.8.8
May 11, 2021 11:10:05.565658092 CEST	53	64267	8.8.8.8	192.168.2.6
May 11, 2021 11:10:06.473062992 CEST	49448	53	192.168.2.6	8.8.8.8
May 11, 2021 11:10:06.521815062 CEST	53	49448	8.8.8.8	192.168.2.6
May 11, 2021 11:10:07.315968037 CEST	60342	53	192.168.2.6	8.8.8.8
May 11, 2021 11:10:07.366607904 CEST	53	60342	8.8.8.8	192.168.2.6
May 11, 2021 11:10:08.172081947 CEST	61346	53	192.168.2.6	8.8.8.8
May 11, 2021 11:10:08.222429991 CEST	53	61346	8.8.8.8	192.168.2.6
May 11, 2021 11:10:09.185693026 CEST	51774	53	192.168.2.6	8.8.8.8
May 11, 2021 11:10:09.235651016 CEST	53	51774	8.8.8.8	192.168.2.6
May 11, 2021 11:10:12.379355907 CEST	56023	53	192.168.2.6	8.8.8.8
May 11, 2021 11:10:12.445902109 CEST	53	56023	8.8.8.8	192.168.2.6
May 11, 2021 11:11:01.546735048 CEST	58384	53	192.168.2.6	8.8.8.8
May 11, 2021 11:11:01.606127977 CEST	53	58384	8.8.8.8	192.168.2.6
May 11, 2021 11:11:56.163331985 CEST	60261	53	192.168.2.6	8.8.8.8
May 11, 2021 11:11:56.240215063 CEST	53	60261	8.8.8.8	192.168.2.6
May 11, 2021 11:12:09.364795923 CEST	56061	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:09.416450024 CEST	53	56061	8.8.8.8	192.168.2.6
May 11, 2021 11:12:13.470910072 CEST	58336	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:13.550908089 CEST	53	58336	8.8.8.8	192.168.2.6
May 11, 2021 11:12:14.031019926 CEST	53781	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:14.105607033 CEST	53	53781	8.8.8.8	192.168.2.6
May 11, 2021 11:12:14.831053019 CEST	54064	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:14.882730961 CEST	53	54064	8.8.8.8	192.168.2.6
May 11, 2021 11:12:16.026129007 CEST	52811	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:16.076328039 CEST	53	52811	8.8.8.8	192.168.2.6
May 11, 2021 11:12:16.941219091 CEST	55299	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:17.005312920 CEST	53	55299	8.8.8.8	192.168.2.6
May 11, 2021 11:12:17.129851103 CEST	63745	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:17.178631067 CEST	53	63745	8.8.8.8	192.168.2.6
May 11, 2021 11:12:18.321643114 CEST	50055	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:18.373451948 CEST	53	50055	8.8.8.8	192.168.2.6
May 11, 2021 11:12:19.467077017 CEST	61374	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:19.518699884 CEST	53	61374	8.8.8.8	192.168.2.6
May 11, 2021 11:12:21.247014046 CEST	50339	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:21.301250935 CEST	53	50339	8.8.8.8	192.168.2.6
May 11, 2021 11:12:24.820668936 CEST	63307	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:24.873788118 CEST	53	63307	8.8.8.8	192.168.2.6
May 11, 2021 11:12:25.939068079 CEST	49694	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:25.987807989 CEST	53	49694	8.8.8.8	192.168.2.6
May 11, 2021 11:12:27.270266056 CEST	54982	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:27.319264889 CEST	53	54982	8.8.8.8	192.168.2.6
May 11, 2021 11:12:42.907170057 CEST	50010	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:42.967122078 CEST	53	50010	8.8.8.8	192.168.2.6
May 11, 2021 11:12:44.360722065 CEST	63718	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:44.412343025 CEST	53	63718	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:12:45.587485075 CEST	62116	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:45.647985935 CEST	53	62116	8.8.8.8	192.168.2.6
May 11, 2021 11:12:45.865833044 CEST	63816	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:45.916495085 CEST	53	63816	8.8.8.8	192.168.2.6
May 11, 2021 11:12:50.559823990 CEST	55014	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:50.628758907 CEST	53	55014	8.8.8.8	192.168.2.6
May 11, 2021 11:12:53.348803043 CEST	62208	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:53.413844109 CEST	53	62208	8.8.8.8	192.168.2.6
May 11, 2021 11:12:58.119138956 CEST	57574	53	192.168.2.6	8.8.8.8
May 11, 2021 11:12:58.181350946 CEST	53	57574	8.8.8.8	192.168.2.6
May 11, 2021 11:13:12.908103943 CEST	51818	53	192.168.2.6	8.8.8.8
May 11, 2021 11:13:12.966835022 CEST	53	51818	8.8.8.8	192.168.2.6
May 11, 2021 11:13:13.940148115 CEST	51818	53	192.168.2.6	8.8.8.8
May 11, 2021 11:13:13.998016119 CEST	53	51818	8.8.8.8	192.168.2.6
May 11, 2021 11:13:14.508028984 CEST	56628	53	192.168.2.6	8.8.8.8
May 11, 2021 11:13:14.608186960 CEST	53	56628	8.8.8.8	192.168.2.6
May 11, 2021 11:13:14.986512899 CEST	51818	53	192.168.2.6	8.8.8.8
May 11, 2021 11:13:15.043967009 CEST	53	51818	8.8.8.8	192.168.2.6
May 11, 2021 11:13:15.190351009 CEST	60778	53	192.168.2.6	8.8.8.8
May 11, 2021 11:13:15.330728054 CEST	53	60778	8.8.8.8	192.168.2.6
May 11, 2021 11:13:15.921439886 CEST	53799	53	192.168.2.6	8.8.8.8
May 11, 2021 11:13:16.058612108 CEST	53	53799	8.8.8.8	192.168.2.6
May 11, 2021 11:13:17.004277945 CEST	51818	53	192.168.2.6	8.8.8.8
May 11, 2021 11:13:17.061121941 CEST	53	51818	8.8.8.8	192.168.2.6
May 11, 2021 11:13:21.021867037 CEST	51818	53	192.168.2.6	8.8.8.8
May 11, 2021 11:13:21.079363108 CEST	53	51818	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 11:12:44.360722065 CEST	192.168.2.6	8.8.8.8	0x5036	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.587485075 CEST	192.168.2.6	8.8.8.8	0xd3a9	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.865833044 CEST	192.168.2.6	8.8.8.8	0x6381	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 11, 2021 11:12:13.550908089 CEST	8.8.8.8	192.168.2.6	0x1017	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:12:44.412343025 CEST	8.8.8.8	192.168.2.6	0x5036	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 11:12:44.412343025 CEST	8.8.8.8	192.168.2.6	0x5036	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 11:12:44.412343025 CEST	8.8.8.8	192.168.2.6	0x5036	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 11:12:44.412343025 CEST	8.8.8.8	192.168.2.6	0x5036	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 11:12:44.412343025 CEST	8.8.8.8	192.168.2.6	0x5036	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 11:12:44.412343025 CEST	8.8.8.8	192.168.2.6	0x5036	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 11, 2021 11:12:44.412343025 CEST	8.8.8.8	192.168.2.6	0x5036	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 11:12:44.412343025 CEST	8.8.8.8	192.168.2.6	0x5036	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.647985935 CEST	8.8.8.8	192.168.2.6	0xd3a9	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:12:45.647985935 CEST	8.8.8.8	192.168.2.6	0xd3a9	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:12:45.647985935 CEST	8.8.8.8	192.168.2.6	0xd3a9	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:12:45.647985935 CEST	8.8.8.8	192.168.2.6	0xd3a9	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:12:45.647985935 CEST	8.8.8.8	192.168.2.6	0xd3a9	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.34	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.647985935 CEST	8.8.8.8	192.168.2.6	0xd3a9	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.50	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.647985935 CEST	8.8.8.8	192.168.2.6	0xd3a9	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.2	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.647985935 CEST	8.8.8.8	192.168.2.6	0xd3a9	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.66	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.916495085 CEST	8.8.8.8	192.168.2.6	0x6381	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:12:45.916495085 CEST	8.8.8.8	192.168.2.6	0x6381	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:12:45.916495085 CEST	8.8.8.8	192.168.2.6	0x6381	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:12:45.916495085 CEST	8.8.8.8	192.168.2.6	0x6381	No error (0)	FRA-efz.ms-acdc.office.com		40.101.12.82	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.916495085 CEST	8.8.8.8	192.168.2.6	0x6381	No error (0)	FRA-efz.ms-acdc.office.com		52.97.179.194	A (IP address)	IN (0x0001)
May 11, 2021 11:12:45.916495085 CEST	8.8.8.8	192.168.2.6	0x6381	No error (0)	FRA-efz.ms-acdc.office.com		52.97.189.98	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	49732	40.97.161.50	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 11:12:44.608804941 CEST	1261	OUT	GET /login/greed/gx9NI4Ybpp/8F85m84ndjn4UwJSZ/KFY_2BxmUPMy/coa0QUktAbb/vjBaicl7yvyNDs/NaAVAq9mPnbNTlKz1AUy2/5aIKWQiZNRBNaijS/Tt5Vo5dnaNIMeJI/Piqfb55cpfCEI8CpHK/_2FWICMIW/YUkQnOfGVld1SPd1rTnm/w0s_2F9NNcplFjkZ_2F/ufX9zF863VCJiOMFbmL1SV/K4t8NhPa8Lg/cl7PdmL.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 11, 2021 11:12:44.792617083 CEST	1262	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/login/greed/gx9NI4Ybpp/8F85m84ndjn4UwJSZ/KFY_2BxmUPMy/coa0QUktAbb/vjBaicl7yvyNDs/NaAVAq9mPnbNTlKz1AUy2/5aIKWQiZNRBNaijS/Tt5Vo5dnaNIMeJI/Piqfb55cpfCEI8CpHK/_2FWICMIW/YUkQnOfGVld1SPd1rTnm/w0s_2F9NNcplFjkZ_2F/ufX9zF863VCJiOMFbmL1SV/K4t8NhPa8Lg/cl7PdmL.gfk Server: Microsoft-IIS/10.0 request-id: 4ac60139-0bd7-4775-a037-e7043fcc077c X-FEServer: MWHPR11CA0031 X-RequestId: 7ab3053c-dc2b-4421-bab2-11ad718bac2f X-Powered-By: ASP.NET X-FEServer: MWHPR11CA0031 Date: Tue, 11 May 2021 09:12:44 GMT Connection: close Content-Length: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6660 Parent PID: 5840

General

Start time:	11:10:12
Start date:	11/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll'
Imagebase:	0xe70000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: 00000001.00000003.662417377.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.724251151.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.662378098.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.662456772.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.662317153.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.662182472.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.662498468.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.662484640.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.662019943.0000000003EA8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6672 Parent PID: 6660

General

Start time:	11:10:12
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.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: 6688 Parent PID: 6660

General

Start time:	11:10:12
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Hundredpopulate@@8

Imagebase:	0xa40000
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: 6700 Parent PID: 6672

General

Start time:	11:10:12
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\609a460e94791.tiff.dll',#1
Imagebase:	0xa40000
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: 00000004.00000003.681209868.0000000005148000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.681069818.0000000005148000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.681166678.0000000005148000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.681184112.0000000005148000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.681198469.0000000005148000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.681099453.0000000005148000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.681146524.0000000005148000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.681124435.0000000005148000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.725706595.0000000005148000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6736 Parent PID: 6660

General

Start time:	11:10:16
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Mark@@12
Imagebase:	0xa40000
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: 6760 Parent PID: 6660

General

Start time:	11:10:20
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\609a460e94791.tiff.dll,Seefit@@8
Imagebase:	0xa40000
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: 5436 Parent PID: 792

General

Start time:	11:12:42
Start date:	11/05/2021
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: 5924 Parent PID: 5436

General

Start time:	11:12:43
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5436 CREDAT:17410 /prefetch:2
Imagebase:	0x3e0000
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