ID: 448650
Sample Name: 945.dll
Cookbook: default.jbs
Time: 15:45:12
Date: 14/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

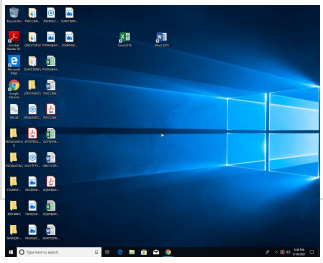
Windows Analysis Report 945.dll

Overview

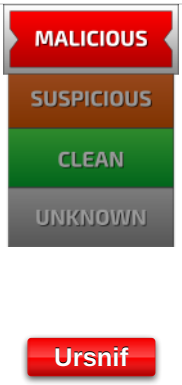
General Information

Sample Name:	945.dll
Analysis ID:	448650
MD5:	9453981ab8e719..
SHA1:	ca0f69ef71bf287…
SHA256:	fa97cd35d76337f..
Tags:	dll gozi
Infos:	

Most interesting Screenshot:



Detection

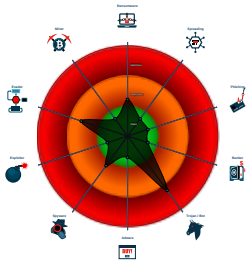


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- 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 locale…
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5904 cmdline: loaddll32.exe 'C:\Users\user\Desktop\945.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5780 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\945.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5516 cmdline: rundll32.exe 'C:\Users\user\Desktop\945.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5784 cmdline: rundll32.exe C:\Users\user\Desktop\945.dll,Clockcondition MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1048 cmdline: rundll32.exe C:\Users\user\Desktop\945.dll,Dogwhen MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1112 cmdline: rundll32.exe C:\Users\user\Desktop\945.dll,Sing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1636 cmdline: rundll32.exe C:\Users\user\Desktop\945.dll,Wholegray MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6084 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5208 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6084 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 3672 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6084 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"ovNAU+HRorLZmwnDvbYFDY7UA+FTIAnF2uJSQd0M+N3ep6CVEhoDrEXACstP09QHK7cBl9nMAaFI1as0K4aXOQKngdScIQbDa3MQ98Ce9MYRMvxGUI05fSIRRFzMVffOXQr97vVUUUPjsYgfkDWS2eKPxSe5dz/pF0mjA0T8ibOLzHmV
Ms4vVv+nwVAw0xpD",
  "c2_domain": [
    "outlook.com",
    "auredosite.club",
    "vuredosite.club"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Copyright Joe Security LLC 2021

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.392687998.0000000002ED8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.391393759.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.391313671.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000002.487967194.0000000002ED8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.391228461.0000000004E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 14 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:

Copyright Joe Security LLC 2021

Yara detected Ursnif

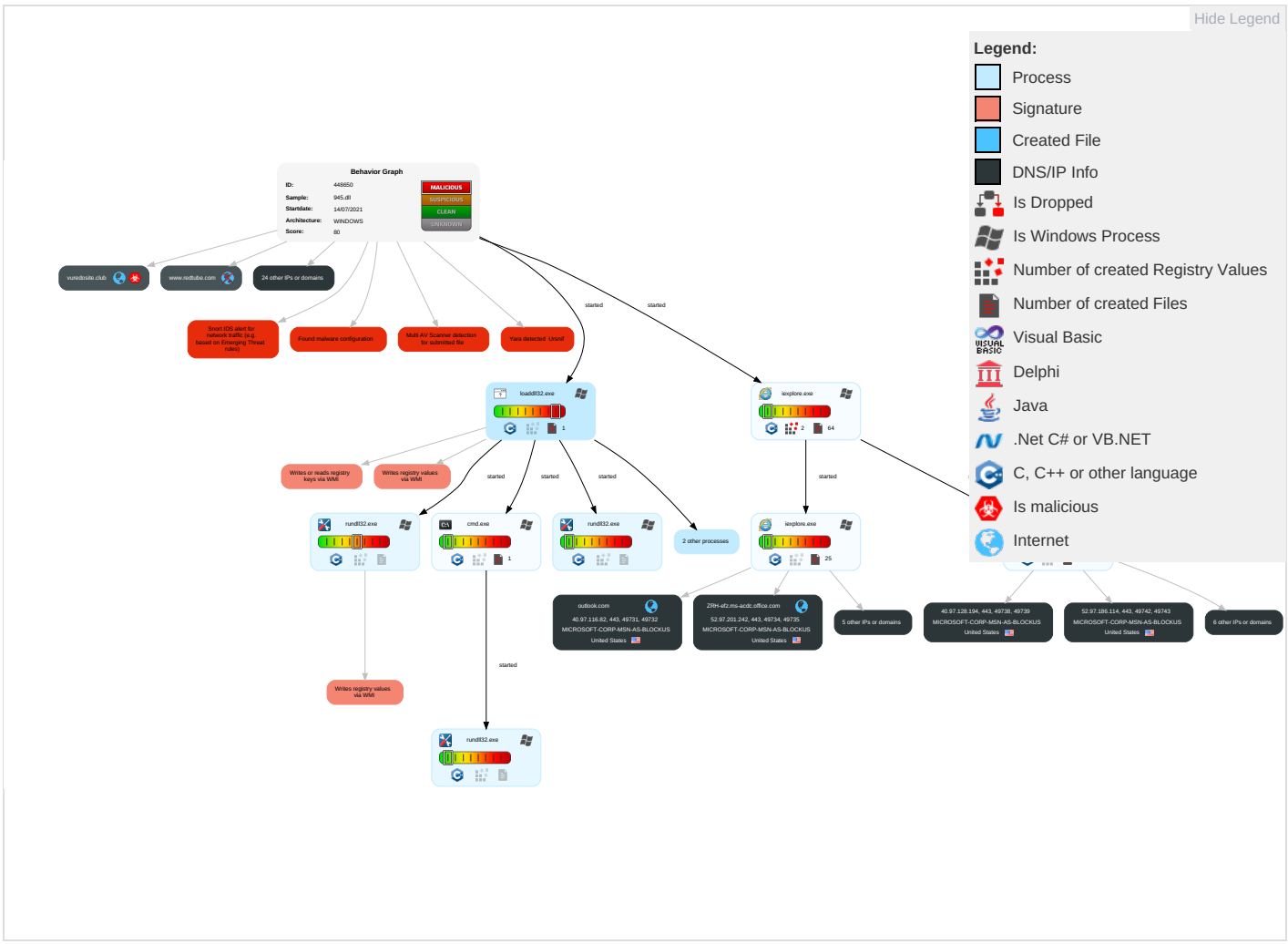
Remote Access Functionality:

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 2	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	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 1	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	File and Directory 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 Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

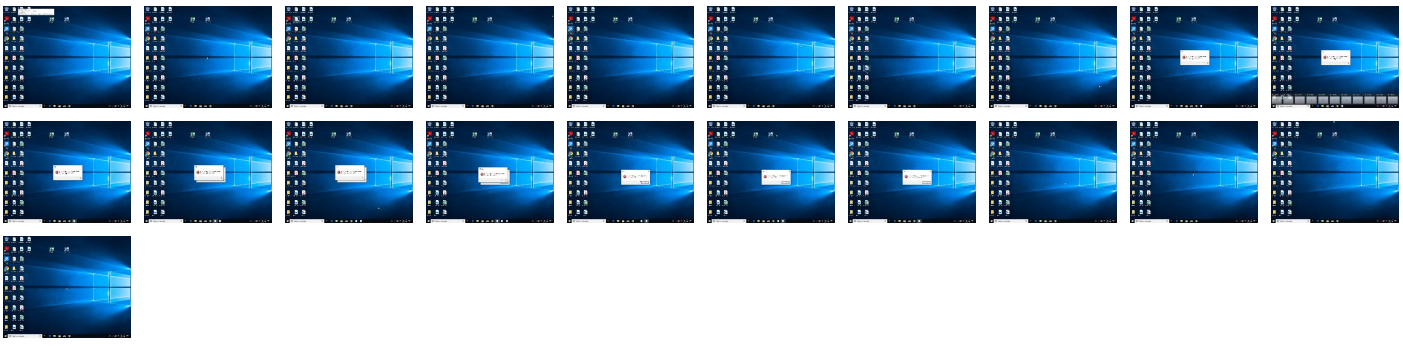
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
945.dll	26%	Metadefender		Browse
945.dll	59%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.960000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.630000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stivers-ricsovers.com	3.65.154.208	true	false		unknown
adpmbtj.com	192.99.16.134	true	false		unknown
ZRH-efz.ms-acdc.office.com	52.97.201.242	true	false		high
stats.l.doubleclick.net	74.125.128.154	true	false		high
redtube.com	66.254.114.238	true	false		high
vip0x055.ssl.rncdn5.com	205.185.208.85	true	false		unknown
vip0x04f.ssl.rncdn5.com	205.185.208.79	true	false		unknown
hubtraffic.com	66.254.114.32	true	false		high
outlook.com	40.97.116.82	true	false		high
ei-ph.rdtcdn.com.sds.rncdn7.com	64.210.135.68	true	false		unknown
ei.rdtcdn.com.sds.rncdn7.com	64.210.135.70	true	false		unknown
ads.trafficjunky.net	66.254.114.38	true	false		high
vuredosite.club	37.120.222.6	true	true		unknown
www.google.ch	172.217.168.3	true	false		high
vip0x08e.ssl.rncdn5.com	205.185.208.142	true	false		unknown
static.trafficjunky.com	unknown	unknown	false		high
www.adpmbtj.com	unknown	unknown	false		unknown
s2.static.cfgr3.com	unknown	unknown	false		unknown
www.redtube.com	unknown	unknown	false		high
di.rdtcdn.com	unknown	unknown	false		high
ei-ph.rdtcdn.com	unknown	unknown	false		high
cdn1d-static-shared.phncdn.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
ht.redtube.com	unknown	unknown	false		high
hw-cdn.trafficjunky.net	unknown	unknown	false		high
www.outlook.com	unknown	unknown	false		high
ei.rdtcdn.com	unknown	unknown	false		high
di-ph.rdtcdn.com	unknown	unknown	false		high
v.vfgte.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://outlook.com/grower/YjL_2BjDOrQaqruzKZl/J5qQT1PxhAWv_2ByqUpS3r/fw5c6vWOUvogF/fDf6v7zv/NA3IFZsX5L82cDak57at8n5/D4Cfgi7tVz/ry3I5zo4IJ_2BIobC/5nWwD7akwp5A/XzqLAJr21mH/cjfkiJFlq9y77G/1bzeLjs6zco1VtNrrz8EL/tJlbiHzqPNR1Mami/EAf48einPLf/Q.grow	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.97.201.242	ZRH-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.97.128.194	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.232.194	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.186.114	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.98.168.178	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.97.116.82	outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Copyright Joe Security LLC 2021

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	448650
Start date:	14.07.2021
Start time:	15:45:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	945.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.winDLL@18/7@34/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.1% (good quality ratio 4.8%) • Quality average: 79.9% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 57% • 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

Simulations

Behavior and APIs

Time	Type	Description
15:47:08	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.97.201.242	http://resa.credit-financebank.com/donc/dcn/?email=bWNnaW5udEByZXNhLm5ldA==	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
52.97.232.194	c36.dll	Get hash	malicious	Browse	
	Signed pages of agreement copy.html	Get hash	malicious	Browse	
	http://YUEipfm.zackgillum.com/%40120%40240%40#james.kelsaw@puc.texas.gov	Get hash	malicious	Browse	
	http://https://microsoft-quarantine.df.r.appspot.com/	Get hash	malicious	Browse	
	Fund Transfer PDF.htm	Get hash	malicious	Browse	
	http://portal.payrolltooling.net/?id=vpqyydl7ZnKtU4usMGPqUQPtxkGlU49Be%2BH%2BAigE5ucTWat3Eej8US2xdckdOu0iDpwQIwMYKl9DLP2pKOIwIWa7isWu4stPeMJ%2BbSSC%2BrsVtg8U%2BWD1tF4Bc3%2FtEr3hJI4S3OomSDlwnU2PwUDgbmdkRVrT8Jiy8Xe4bfQ0dyp5k2o%2Bf2eztEQzNsZlKz0xjWSRZcdjYCg9vWmNNNSvSwsWNybr8UBeONKYmj4PdCOwhNBWdvur%2BK4Wx1bqcPE26q7z8kpyQ4hJ2vOCvXmdlnZ37w0%2BAGvM3H2V03OaxIsBHrlCuyiPhQWq8qdKOB4lg1EmFibK759dnK%2FawF2z6INf5lJhbtrbLVkWA6i%2FuckBPOJvVXHWYj5SHhB8X%2FZz	Get hash	malicious	Browse	
	P.I Officewears 28.07.2020.exe	Get hash	malicious	Browse	
	http://wcladr.atoo.xyz/%407499%401289%40#rhys.hodge@2sfg.com	Get hash	malicious	Browse	
	http://https://angularjs-xcyejc.stackblitz.io/	Get hash	malicious	Browse	
	http://https://office365-0nedrive-portal.el.r.appspot.com/	Get hash	malicious	Browse	
	http://https://austeamatic-my.sharepoint.com/:f:/g/personal/wspence_steamatic_com_au/ElyRlyMAVJtHn6FFuMTMYowBrq7r9BGosqf6VblEm4AzkA?e=S5Qh6c	Get hash	malicious	Browse	
	http://https://xlelectricals.com/dolex/offices/index.php	Get hash	malicious	Browse	
	http://https://firebasestorage.googleapis.com/v0/b/j3q3d3sqsuuser.appspot.com/o/index.htm?alt=media&token=a6ff4f2d-2706-4fc4-bf56-5796926e37ef#cathyc@stockland.com.au	Get hash	malicious	Browse	
	http://https://jetlow.z19.web.core.windows.net/#is@loreal.com	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ZRH-efz.ms-acdc.office.com	c36.dll	Get hash	malicious	Browse	• 52.97.186.114
	c36.dll	Get hash	malicious	Browse	• 52.98.163.18
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 52.97.232.194
	PI_DRAFT.exe	Get hash	malicious	Browse	• 52.97.186.114
	moog_invoice_Wednesday 02242021._xslx.hTML	Get hash	malicious	Browse	• 52.97.201.210
	http://https://app.box.com/s/yihmp2wywbz9lgdbg26g3tc1piwkalab	Get hash	malicious	Browse	• 52.97.232.210
	http://resa.credit-financebank.com/donc/dcn/?email=bWNnaW5udEByZXNhLm5ldA==	Get hash	malicious	Browse	• 52.97.201.242
	http://https://loginpro-288816.ew.r.appspot.com/#joshua.kwon@ttc.ca	Get hash	malicious	Browse	• 52.97.186.98
	http://YUEipfm.zackgillum.com/%40120%40240%40#james.kelsaw@puc.texas.gov	Get hash	malicious	Browse	• 52.97.232.194
	http://https://microsoft-quarantine.df.r.appspot.com/	Get hash	malicious	Browse	• 52.97.232.194
	http://https://storage.googleapis.com/atotalled-370566990/index.html	Get hash	malicious	Browse	• 52.97.186.18
	http://https://login-microsoft-office365-auth.el.r.appspot.com/login.microsoftonline.com/common/oauth2/authorize=vNews2&email=microsoftonline.com/common/oauth2/authorize&hashed_email=Y7XY6XCZJ3R4T4MN&utm_campaign=phx_trigger_uk_pop_email4&utm_source=photobox&utm_medium=email&uid=4978854645473&brandName=Photobox#helen@rhdb.com.au	Get hash	malicious	Browse	• 52.97.232.242
	http://https://clicktime.symantec.com/3LNDmLN9vLnK1LqGUDBbkAD6H2?u=https%3A%2F%2Foutlook.office.com%2Fmail%2Fsearch%2Fid%2Fnscglobal.com	Get hash	malicious	Browse	• 52.97.232.226
	http://https://luminous-cubist-288118.df.r.appspot.com/#lilja.b.einarsdottir@landsbankinn.is	Get hash	malicious	Browse	• 52.97.232.226

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://u4882271.ct.sendgrid.net/ls/click?upn=YFyCGXB2k7XEs51EAWvRp-2BQ6xaP5-2Bxv1vyI4slTyTp6VhtJSyiu7Ungt4CUf7KdGeEBPZ7lJ0WMtGrW3-2F8wXB5klqpkSCZwccYVceognA2U-3D57Rw_kfZ8cLppmcXDuIHKWdMrLPt30SkBa8ipQz83IjjYGp9c2flQixqYXWN470AqCFO8g1yhSwMHhN8-2BJK0vTLNC61PkTeWIrAs821yYsBfCbuclR33OfNLncv-2FtXraICcEYo4WPVv8iupWN7r8K4Ld3UpsglQggrT98vACCXZNhqlBcQYKLRD-2BBljUb02MnMpFHKiH9-2BP5uH3bAOFC4VOgSpVi86N1p2cxRMZF5Xkh4ZdU-3D	Get hash	malicious	Browse	• 52.97.186.114
	http://https://share-ointonlinekcjl5cj5k.et.r.appspot.com/#I.Artolli@sbm.mc	Get hash	malicious	Browse	• 52.97.186.18
	Fund Transfer PDF.htm	Get hash	malicious	Browse	• 52.97.232.194
	http://outlook.com/owa/airmasteraustralia.onmicrosoft.com	Get hash	malicious	Browse	• 52.97.232.226
	http://portal.payrolltooling.net/?id=vpqyydl7ZnKtU4usMGPqUQPtxkGlU49Be%2BH%2BAigE5ucTWat3Eej8US2xdckdOu0iDpwQIwMYKl9DLP2pKOlwIWa7isWu4stPeMJ%2BbSSC%2BrsVtg8U%2BWD1tF4Bc3%2FtEr3hJI4S3OomSDlwnU2PwUDgbmdkRVrT8Jiy8Xe4bfQ0dyp5k2o%2Bf2eztEQzNsZlKz0xjWSRZcdjYCg9vWmNNNSvSwsWNybr8UBeONKYmj4PdCOwhNBWdvur%2BK4Wx1bqcPE26q7z8kpyQ4hJ2vOCvXmdlnZ37w0%2BAGvM3H2V03OaxIsBHrlCuyiPhQWq8qdKOB4lg1EmFibK759dnK%2FawF2z6INf5IJhbtrbLVkWA6i%2FuckBPOJvVXHWYj5SHhB8X%2FZz	Get hash	malicious	Browse	• 52.97.232.194
	okayfreedomwr.exe	Get hash	malicious	Browse	• 52.97.232.194
stats.l.doubleclick.net	60e40fb428612.dll	Get hash	malicious	Browse	• 142.250.102.155
	TestTakerSBBrowser.exe	Get hash	malicious	Browse	• 74.125.133.155
	vNiyRd4GcH.exe	Get hash	malicious	Browse	• 108.177.15.154
	sf0X1hMF0g.doc	Get hash	malicious	Browse	• 74.125.140.157
	sf0X1hMF0g.doc	Get hash	malicious	Browse	• 74.125.140.155
	DocuSign-June-SOA-Dues.261.htm	Get hash	malicious	Browse	• 74.125.140.157
	XqnM8G36Ih.exe	Get hash	malicious	Browse	• 74.125.140.157
	bmaphis@cardinaltek.com_16465506 AMDocAtt.HTML	Get hash	malicious	Browse	• 74.125.140.154
	Global _Transport NZ..xlsx	Get hash	malicious	Browse	• 74.125.140.157
	Global _Transport NZ..xlsx	Get hash	malicious	Browse	• 74.125.140.156
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 74.125.140.157
	HRXoZLG4ym.exe	Get hash	malicious	Browse	• 74.125.140.155
	MacKeeper.5.4.pkg	Get hash	malicious	Browse	• 142.250.27.154
	Hngx5CdG2D.exe	Get hash	malicious	Browse	• 74.125.140.154
	5474_-_Test_Call_Procedure_4.2.docx	Get hash	malicious	Browse	• 74.125.140.154
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 142.251.5.154
	crt9O3URua.exe	Get hash	malicious	Browse	• 142.250.102.154
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 142.250.102.157
	Ref#Doc30504871 Wyg.htm	Get hash	malicious	Browse	• 173.194.76.156
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 74.125.140.157
stivers-ricsovers.com	609110f2d14a6.dll	Get hash	malicious	Browse	• 18.195.174.160

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	uLTvM5APNY.exe	Get hash	malicious	Browse	• 104.47.54.36
	X7FqAeP3oE.exe	Get hash	malicious	Browse	• 104.42.151.234
	8944848MNBV.exe	Get hash	malicious	Browse	• 23.101.8.193
	5odgesjcMa.exe	Get hash	malicious	Browse	• 168.61.161.212
	Horodlsjjdrxysbousfnmraroywkyeqrjq.exe	Get hash	malicious	Browse	• 20.80.51.178
	Hond.exe	Get hash	malicious	Browse	• 168.61.161.212
	6dCudgmxKY.exe	Get hash	malicious	Browse	• 104.42.151.234
	SIeDLrXyLs.exe	Get hash	malicious	Browse	• 20.194.35.6
	cCEP3pyVp8.exe	Get hash	malicious	Browse	• 13.64.90.137
	codes.zip.exe	Get hash	malicious	Browse	• 52.239.214.132
	Qyqcfpjnkpfztrximioqcwcfursbkeatda.exe	Get hash	malicious	Browse	• 20.80.30.45
	HQZzLlAZjR.exe	Get hash	malicious	Browse	• 20.151.200.9
	HQZzLlAZjR.exe	Get hash	malicious	Browse	• 20.151.200.9
	31Ov8DqdkE.exe	Get hash	malicious	Browse	• 157.56.161.162
	c36.dll	Get hash	malicious	Browse	• 52.97.232.194
	c36.dll	Get hash	malicious	Browse	• 52.98.163.18
	2oxhsHaX3D.exe	Get hash	malicious	Browse	• 13.107.4.50

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iKcDLx5Wxc.exe	Get hash	malicious	Browse	• 104.43.139.144
	r6.zip.exe	Get hash	malicious	Browse	• 52.239.214.132
	recovered_bin2	Get hash	malicious	Browse	• 52.228.135.155
MICROSOFT-CORP-MSN-AS-BLOCKUS	uLTvM5APNY.exe	Get hash	malicious	Browse	• 104.47.54.36
	X7FqAeP3oE.exe	Get hash	malicious	Browse	• 104.42.151.234
	8944848MNBV.exe	Get hash	malicious	Browse	• 23.101.8.193
	5odgesjcMa.exe	Get hash	malicious	Browse	• 168.61.161.212
	Horodlsjjdrxysbousfnmraroywkyeqrjq.exe	Get hash	malicious	Browse	• 20.80.51.178
	Hond.exe	Get hash	malicious	Browse	• 168.61.161.212
	6dCudgmxKY.exe	Get hash	malicious	Browse	• 104.42.151.234
	SleDLrXyLs.exe	Get hash	malicious	Browse	• 20.194.35.6
	cCEP3pyVp8.exe	Get hash	malicious	Browse	• 13.64.90.137
	codes.zip.exe	Get hash	malicious	Browse	• 52.239.214.132
	Qyqcfpjnkpfztrximioqcwcfursbkeatda.exe	Get hash	malicious	Browse	• 20.80.30.45
	HQZzLlAZjR.exe	Get hash	malicious	Browse	• 20.151.200.9
	HQZzLlAZjR.exe	Get hash	malicious	Browse	• 20.151.200.9
	31Ov8DqdkE.exe	Get hash	malicious	Browse	• 157.56.161.162
	c36.dll	Get hash	malicious	Browse	• 52.97.232.194
	c36.dll	Get hash	malicious	Browse	• 52.98.163.18
	2oxhsHaX3D.exe	Get hash	malicious	Browse	• 13.107.4.50
	iKcDLx5Wxc.exe	Get hash	malicious	Browse	• 104.43.139.144
	r6.zip.exe	Get hash	malicious	Browse	• 52.239.214.132
	recovered_bin2	Get hash	malicious	Browse	• 52.228.135.155

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7370D51F-E4F5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.007817288091259
Encrypted:	false
SSDEEP:	192:rZZeZu2TWetyf0NMPjPxPAYMP2TBVKAu4llg:rPKFqewRPjPxPMP2TC4F
MD5:	72DFFC63D7B320FF56607CACBBF2D659
SHA1:	9694D0EF54C82CAC4D3C55740C7C9298B725FE31
SHA-256:	87260A3937BAA49E596D024895EE0EADC06DF10892C4CEFAEE87B8C557233A42
SHA-512:	B78566E638A0FA880AB105B031320A876761CDDE77F5F77762EA39FAB72C0354162E1CCEEE53864E89B37A097BA9F08E59D33C2F6AE288D6E235AA0F749E311A
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7370D521-E4F5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.839005711968297
Encrypted:	false
SSDEEP:	96:rWZtQd6jBSZjN2hWfMHigB96Juge/GxgB96Juge/g96ZA:rWZtQd6jkZjN2hWfMHigWlxgWuA
MD5:	6AB6BAE717B506BF99138EAD4712FD5D
SHA1:	D968B18FA142DFAD6808349EE20F52AABF8A46F5

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7370D521-E4F5-11EB-90E4-ECF4BB862DED}.dat	
SHA-256:	B60F5051287D0F98A62928ABBD2B25CA46E8FACC716BCD585C41CBE70447C925
SHA-512:	CD3011896E2A9477020EEA8AA7A7C3241FE51AB12F6C011F0068BAFF675CFF1A72D104631751416CAB5B4A24D297B2ADC156F94B5B30A911810AFCD132EE4F0
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7370D523-E4F5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27436
Entropy (8bit):	1.8611245040893345
Encrypted:	false
SSDEEP:	96:rKZtQZ67BSijh2FW4MW+8BszVMkMPx8BszVMkMwszFCA:rKZtQZ67kijh2FW4MW+8Wzsx8WzezFCA
MD5:	B45BE5E0689CA52E7AA317477CEAB2EB
SHA1:	0D308F7400E760E9053A8DC45D37FD4746C832A8
SHA-256:	C205717F2E113190755FCD2A714B8D891B4045EB9DB81ECB36868D55687B5033
SHA-512:	F3C842EA151F324A2E582FF32F71C8B9B6B2A202D6277F3BA389AD787E9199216849F8B86554B5918114E71F3A10148B87D8103A1114B058E420D34B3DDABE2E
Malicious:	false
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:	dropped
Size (bytes):	89
Entropy (8bit):	4.45974266689267
Encrypted:	false
SSDEEP:	3:oVXUtJf0fBovpEH8JOGXnEtJf0fBovUSX+n:o9UtJsUiqEtJsUU7
MD5:	5AF30AB03EEB684130F909A48D6C87EC
SHA1:	E217A694B2C4E7EA04763EA6A99B9A577652016B
SHA-256:	A743A35C1772ECEAA2F22B3765935A911CA50A23156F04EFC4FBFCC42F8B9F1A
SHA-512:	2813B7FE1FF192128C97894DB317964A66FCB38B7E330EA6A07456BD73BD7FBDF432E9BAA4311FDE3FE0A147DB756EDC53F1C64830D10949FDAE14E38AD52A7
Malicious:	false
Preview:	[2021/07/14 15:47:24.961] Latest deploy version: ..[2021/07/14 15:47:24.961] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF08C928D5E36F5DDB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5978024045945609
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loMpF9loMr9lWMZofjBMjBMRyBMRTTTi:kBqoI7dhjBMjBMRyBMRvO
MD5:	288585C44B20EA24B2FD22E86C0AC593
SHA1:	D72E31BF7599CC277A793D645FECB07371B5E665
SHA-256:	DF52758571E4D35099BAA3057ACE9396DD2FEAA5D9B3EE51698BFF7531350701
SHA-512:	C277CDFDFDD901B86DAF202F718801A410E8B6B23FAFAF37282EDB242C8FFED45D31F59B77B899EB82AC0D8AC6464785A99CEAD24FADE5D13D29126DDC37E94
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF64A2AAB8E5E3DF4B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF64A2AAB8E5E3DF4B.TMP	
Size (bytes):	39769
Entropy (8bit):	0.5967894698585455
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+AGcdGM8BszVMkMC8BszVMkMm8BszVMkM3:kBqoxKAuqR+AGcdGM8WzH8Wzn8Wzs
MD5:	2D85FE4AF6F5C992507FB76E7BDA0792
SHA1:	A279DE73D9632650F4D76CF2FF77FD69FAA6EE06
SHA-256:	90DCAC7CD40AD46F46C4EA799D12DA79C04C0D937AC1195862881314D51EC070
SHA-512:	9E0774C8B71744D0329ECC51355627F3E3B650A8DFDF22470BB1FA39A9A7C312CA637DA93F334FDF2DC4F639C81D0E649B34B0A89019FF2562DD5A7092660B9
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

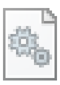
C:\Users\user\AppData\Local\Temp\~DFEA5774EEA628D538.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39633
Entropy (8bit):	0.5703763819497271
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+Z3lUX9gB96Juge/egB96Juge/+gB96Juge/3:kBqoxKAuqR+Z3lUX9gW7gW/gWk
MD5:	438BF405E16CD9C0230E87A245B3986D
SHA1:	3E253609827B74E371E078EE26FEA1E73D6DE489
SHA-256:	E36EBB25504C9233020CB6BBD89F01773C287628FE0BDF189F387E1DCC59E330
SHA-512:	C2BD4B2756B618C0EC6EC5FF881461B78C4EDEEC420699559D3773E444DC5CCC74D80B046A1CDBF830FFCFAB62355A40019A6EDAE1C05E4D3620451ED16F9 5A
Malicious:	false
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):	6.657188224349107
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:	945.dll
File size:	381440
MD5:	9453981ab8e71981bea907b3f2d11395
SHA1:	ca0f69ef71bf287bdd19a8a9811c1f0dd2ff50e6
SHA256:	fa97cd35d76337ff4a523ebdd7f879359a70432a14b7377f 06df29c4679b3f70
SHA512:	7c1dcf301adbda28a202f77d5898215ea7292ea3c1ccfa2 bb8d2af97e417a1e11824c99c878694e972227d3f1038d6 3b5052d670b1aeb8226859a511245406c1
SSDEEP:	6144:vC8nRa6tXFOspzA736NZVeC8i795fubASK9beZT X3l8Eo:J0SVOspFVWi7PWoBeZTX36
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.........~@...... ....D... Rich............PE..L......S...

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x102cd58
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:	0x5396CBB2 [Tue Jun 10 09:11:14 2014 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:	4c29865e356872ef0757b58734cbbb11

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4211f	0x42200	False	0.619808896503	data	6.63192382314	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x44000	0x16172	0x16200	False	0.578919491525	data	5.90225736165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5b000	0x980ec	0x1c00	False	0.316824776786	data	3.9217328811	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xf4000	0x1e0	0x200	False	0.529296875	data	4.724728912	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf5000	0x2b1c	0x2c00	False	0.760919744318	data	6.67218651592	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

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
07/14/21-15:47:26.154158	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49731	80	192.168.2.3	40.97.116.82
07/14/21-15:48:10.427089	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49749	80	192.168.2.3	37.120.222.6
07/14/21-15:48:10.427089	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49749	80	192.168.2.3	37.120.222.6
07/14/21-15:48:10.738630	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49752	80	192.168.2.3	37.120.222.6

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 14, 2021 15:47:25.931644917 CEST	192.168.2.3	8.8.8.8	0xae44	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:26.955091953 CEST	192.168.2.3	8.8.8.8	0xf6af	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.053947926 CEST	192.168.2.3	8.8.8.8	0xcd84	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.307626009 CEST	192.168.2.3	8.8.8.8	0x9da2	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.849246025 CEST	192.168.2.3	8.8.8.8	0xa15c	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.953054905 CEST	192.168.2.3	8.8.8.8	0x88c5	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:10.365509987 CEST	192.168.2.3	8.8.8.8	0x1382	Standard query (0)	vuredosite.club	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:10.698997974 CEST	192.168.2.3	8.8.8.8	0x246e	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:10.699883938 CEST	192.168.2.3	8.8.8.8	0x760d	Standard query (0)	vuredosite.club	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:10.790649891 CEST	192.168.2.3	8.8.8.8	0x28f8	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.821281910 CEST	192.168.2.3	8.8.8.8	0x5a66	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.827414036 CEST	192.168.2.3	8.8.8.8	0xf681	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.834091902 CEST	192.168.2.3	8.8.8.8	0xb65c	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.850749016 CEST	192.168.2.3	8.8.8.8	0x65f2	Standard query (0)	di.rdtcdn.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.873614073 CEST	192.168.2.3	8.8.8.8	0xaa8c	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.877441883 CEST	192.168.2.3	8.8.8.8	0xad42	Standard query (0)	di.rdtcdn.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.880283117 CEST	192.168.2.3	8.8.8.8	0x6d41	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.947179079 CEST	192.168.2.3	8.8.8.8	0x7a2	Standard query (0)	ht.redtube.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.983000994 CEST	192.168.2.3	8.8.8.8	0xfad8	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.987709045 CEST	192.168.2.3	8.8.8.8	0x15e3	Standard query (0)	ht.redtube.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.067157030 CEST	192.168.2.3	8.8.8.8	0x9ffa	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.228458881 CEST	192.168.2.3	8.8.8.8	0x330d	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.684083939 CEST	192.168.2.3	8.8.8.8	0x6311	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.879894972 CEST	192.168.2.3	8.8.8.8	0x852	Standard query (0)	di-ph.rdtcdn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 14, 2021 15:48:12.907186985 CEST	192.168.2.3	8.8.8.8	0xb4b3	Standard query (0)	ei-ph.rdtcdn.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.987462044 CEST	192.168.2.3	8.8.8.8	0xf5f8	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.028877020 CEST	192.168.2.3	8.8.8.8	0xa57d	Standard query (0)	hw-cdn.trafficjunky.net	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.032063007 CEST	192.168.2.3	8.8.8.8	0xe7a8	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.103856087 CEST	192.168.2.3	8.8.8.8	0x6561	Standard query (0)	www.adpmbtj.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.141252041 CEST	192.168.2.3	8.8.8.8	0xd35	Standard query (0)	hw-cdn.trafficjunky.net	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.144398928 CEST	192.168.2.3	8.8.8.8	0xa895	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.490489006 CEST	192.168.2.3	8.8.8.8	0x1fb9	Standard query (0)	v.vfgte.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.665746927 CEST	192.168.2.3	8.8.8.8	0x4639	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.952934027 CEST	192.168.2.3	8.8.8.8	0x901b	Standard query (0)	s2.static.cfgr3.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 14, 2021 15:47:06.327312946 CEST	8.8.8.8	192.168.2.3	0xd187	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:25.944113970 CEST	8.8.8.8	192.168.2.3	0xae44	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:25.944113970 CEST	8.8.8.8	192.168.2.3	0xae44	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:25.944113970 CEST	8.8.8.8	192.168.2.3	0xae44	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:25.944113970 CEST	8.8.8.8	192.168.2.3	0xae44	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:25.944113970 CEST	8.8.8.8	192.168.2.3	0xae44	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:25.944113970 CEST	8.8.8.8	192.168.2.3	0xae44	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:25.944113970 CEST	8.8.8.8	192.168.2.3	0xae44	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:25.944113970 CEST	8.8.8.8	192.168.2.3	0xae44	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:26.968219995 CEST	8.8.8.8	192.168.2.3	0xf6af	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:26.968219995 CEST	8.8.8.8	192.168.2.3	0xf6af	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:26.968219995 CEST	8.8.8.8	192.168.2.3	0xf6af	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:26.968219995 CEST	8.8.8.8	192.168.2.3	0xf6af	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:26.968219995 CEST	8.8.8.8	192.168.2.3	0xf6af	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.242	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:26.968219995 CEST	8.8.8.8	192.168.2.3	0xf6af	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:26.968219995 CEST	8.8.8.8	192.168.2.3	0xf6af	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.186.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:26.968219995 CEST	8.8.8.8	192.168.2.3	0xf6af	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.186.114	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 14, 2021 15:47:27.066414118 CEST	8.8.8.8	192.168.2.3	0xcd84	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.066414118 CEST	8.8.8.8	192.168.2.3	0xcd84	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.066414118 CEST	8.8.8.8	192.168.2.3	0xcd84	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.066414118 CEST	8.8.8.8	192.168.2.3	0xcd84	No error (0)	ZRH-efz.ms-acdc.office.com		52.98.168.178	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.066414118 CEST	8.8.8.8	192.168.2.3	0xcd84	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.242	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.066414118 CEST	8.8.8.8	192.168.2.3	0xcd84	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.226	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.066414118 CEST	8.8.8.8	192.168.2.3	0xcd84	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.194	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.320375919 CEST	8.8.8.8	192.168.2.3	0x9da2	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.320375919 CEST	8.8.8.8	192.168.2.3	0x9da2	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.320375919 CEST	8.8.8.8	192.168.2.3	0x9da2	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.320375919 CEST	8.8.8.8	192.168.2.3	0x9da2	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.320375919 CEST	8.8.8.8	192.168.2.3	0x9da2	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.320375919 CEST	8.8.8.8	192.168.2.3	0x9da2	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.320375919 CEST	8.8.8.8	192.168.2.3	0x9da2	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.320375919 CEST	8.8.8.8	192.168.2.3	0x9da2	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.862534046 CEST	8.8.8.8	192.168.2.3	0xa15c	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.862534046 CEST	8.8.8.8	192.168.2.3	0xa15c	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.862534046 CEST	8.8.8.8	192.168.2.3	0xa15c	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.862534046 CEST	8.8.8.8	192.168.2.3	0xa15c	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.862534046 CEST	8.8.8.8	192.168.2.3	0xa15c	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.194	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.862534046 CEST	8.8.8.8	192.168.2.3	0xa15c	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.862534046 CEST	8.8.8.8	192.168.2.3	0xa15c	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.862534046 CEST	8.8.8.8	192.168.2.3	0xa15c	No error (0)	ZRH-efz.ms-acdc.office.com		52.98.163.18	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.965689898 CEST	8.8.8.8	192.168.2.3	0x88c5	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.965689898 CEST	8.8.8.8	192.168.2.3	0x88c5	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:27.965689898 CEST	8.8.8.8	192.168.2.3	0x88c5	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 14, 2021 15:47:27.965689898 CEST	8.8.8.8	192.168.2.3	0x88c5	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.186.114	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.965689898 CEST	8.8.8.8	192.168.2.3	0x88c5	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.965689898 CEST	8.8.8.8	192.168.2.3	0x88c5	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.226	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:27.965689898 CEST	8.8.8.8	192.168.2.3	0x88c5	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:10.393398046 CEST	8.8.8.8	192.168.2.3	0x1382	No error (0)	vuredosite.club		37.120.222.6	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:10.713897943 CEST	8.8.8.8	192.168.2.3	0x760d	No error (0)	vuredosite.club		37.120.222.6	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:10.721282005 CEST	8.8.8.8	192.168.2.3	0x246e	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:10.721282005 CEST	8.8.8.8	192.168.2.3	0x246e	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:10.803733110 CEST	8.8.8.8	192.168.2.3	0x28f8	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:10.803733110 CEST	8.8.8.8	192.168.2.3	0x28f8	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.834767103 CEST	8.8.8.8	192.168.2.3	0x5a66	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:11.834767103 CEST	8.8.8.8	192.168.2.3	0x5a66	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.847233057 CEST	8.8.8.8	192.168.2.3	0xb65c	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:11.847233057 CEST	8.8.8.8	192.168.2.3	0xb65c	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.863822937 CEST	8.8.8.8	192.168.2.3	0x65f2	No error (0)	di.rdtcdn.com	cds.e9q5t8x5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:11.891727924 CEST	8.8.8.8	192.168.2.3	0xad42	No error (0)	di.rdtcdn.com	cds.e9q5t8x5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:11.892944098 CEST	8.8.8.8	192.168.2.3	0x6d41	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:11.892944098 CEST	8.8.8.8	192.168.2.3	0x6d41	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.960560083 CEST	8.8.8.8	192.168.2.3	0x7a2	No error (0)	ht.redtube.com	hubtraffic.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:11.960560083 CEST	8.8.8.8	192.168.2.3	0x7a2	No error (0)	hubtraffic.com		66.254.114.32	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:11.995903969 CEST	8.8.8.8	192.168.2.3	0xfad8	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:11.995903969 CEST	8.8.8.8	192.168.2.3	0xfad8	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.000539064 CEST	8.8.8.8	192.168.2.3	0x15e3	No error (0)	ht.redtube.com	hubtraffic.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:12.000539064 CEST	8.8.8.8	192.168.2.3	0x15e3	No error (0)	hubtraffic.com		66.254.114.32	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.079461098 CEST	8.8.8.8	192.168.2.3	0xf681	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:12.079461098 CEST	8.8.8.8	192.168.2.3	0xf681	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 14, 2021 15:48:12.079461098 CEST	8.8.8.8	192.168.2.3	0xf681	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.079461098 CEST	8.8.8.8	192.168.2.3	0xf681	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.083242893 CEST	8.8.8.8	192.168.2.3	0x9ffa	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:12.083242893 CEST	8.8.8.8	192.168.2.3	0x9ffa	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.125993013 CEST	8.8.8.8	192.168.2.3	0xaa8c	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:12.125993013 CEST	8.8.8.8	192.168.2.3	0xaa8c	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.125993013 CEST	8.8.8.8	192.168.2.3	0xaa8c	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.125993013 CEST	8.8.8.8	192.168.2.3	0xaa8c	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.242551088 CEST	8.8.8.8	192.168.2.3	0x330d	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:12.242551088 CEST	8.8.8.8	192.168.2.3	0x330d	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.699738979 CEST	8.8.8.8	192.168.2.3	0x6311	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:12.699738979 CEST	8.8.8.8	192.168.2.3	0x6311	No error (0)	stats.l.doubleclick.net		74.125.128.154	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.699738979 CEST	8.8.8.8	192.168.2.3	0x6311	No error (0)	stats.l.doubleclick.net		74.125.128.156	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.699738979 CEST	8.8.8.8	192.168.2.3	0x6311	No error (0)	stats.l.doubleclick.net		74.125.128.157	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.699738979 CEST	8.8.8.8	192.168.2.3	0x6311	No error (0)	stats.l.doubleclick.net		74.125.128.155	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:12.893663883 CEST	8.8.8.8	192.168.2.3	0x852	No error (0)	di-ph.rdtcdn.com	cds.b8w3s7t8.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:13.014607906 CEST	8.8.8.8	192.168.2.3	0xf5f8	No error (0)	www.google.ch		172.217.168.3	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.041376114 CEST	8.8.8.8	192.168.2.3	0xa57d	No error (0)	hw-cdn.trafficjunky.net	vip0x055.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:13.041376114 CEST	8.8.8.8	192.168.2.3	0xa57d	No error (0)	vip0x055.ssl.rncdn5.com		205.185.208.85	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.045175076 CEST	8.8.8.8	192.168.2.3	0xe7a8	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.117070913 CEST	8.8.8.8	192.168.2.3	0x6561	No error (0)	www.adpmbtj.com	adpmbtj.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:13.117070913 CEST	8.8.8.8	192.168.2.3	0x6561	No error (0)	adpmbtj.com		192.99.16.134	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.117070913 CEST	8.8.8.8	192.168.2.3	0x6561	No error (0)	adpmbtj.com		192.99.16.68	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.117070913 CEST	8.8.8.8	192.168.2.3	0x6561	No error (0)	adpmbtj.com		142.4.219.200	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.117070913 CEST	8.8.8.8	192.168.2.3	0x6561	No error (0)	adpmbtj.com		192.99.16.137	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.117070913 CEST	8.8.8.8	192.168.2.3	0x6561	No error (0)	adpmbtj.com		192.99.16.114	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 14, 2021 15:48:13.117070913 CEST	8.8.8.8	192.168.2.3	0x6561	No error (0)	adpmbtj.com		192.99.16.132	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.154074907 CEST	8.8.8.8	192.168.2.3	0xd35	No error (0)	hw-cdn.traffficjunky.net	vip0x055.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:13.154074907 CEST	8.8.8.8	192.168.2.3	0xd35	No error (0)	vip0x055.ssl.rncdn5.com		205.185.208.85	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.157198906 CEST	8.8.8.8	192.168.2.3	0xa895	No error (0)	ads.traffficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.163647890 CEST	8.8.8.8	192.168.2.3	0xb4b3	No error (0)	ei-ph.rdtcdn.com	ei-ph.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:13.163647890 CEST	8.8.8.8	192.168.2.3	0xb4b3	No error (0)	ei-ph.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.163647890 CEST	8.8.8.8	192.168.2.3	0xb4b3	No error (0)	ei-ph.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.163647890 CEST	8.8.8.8	192.168.2.3	0xb4b3	No error (0)	ei-ph.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.510392904 CEST	8.8.8.8	192.168.2.3	0x1fb9	No error (0)	v.vfgte.com	stivers-ricsovers.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:13.510392904 CEST	8.8.8.8	192.168.2.3	0x1fb9	No error (0)	stivers-ricsovers.com		3.65.154.208	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.510392904 CEST	8.8.8.8	192.168.2.3	0x1fb9	No error (0)	stivers-ricsovers.com		18.195.174.160	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.678721905 CEST	8.8.8.8	192.168.2.3	0x4639	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:48:13.678721905 CEST	8.8.8.8	192.168.2.3	0x4639	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Jul 14, 2021 15:48:13.966341019 CEST	8.8.8.8	192.168.2.3	0x901b	No error (0)	s2.static.cfgr3.com	vip0x011.ssl.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- outlook.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49731	40.97.116.82	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 14, 2021 15:47:26.154158115 CEST	1351	OUT	GET /grower/YjL_2BjDOrQaqruzKZl/J5qQT1PxhAWv_2ByqUpS3r/fw5c6vWOUvogF/fDf6v7zv/NA3IFZsX5L82cDak57at8n5/D4Cfgi7tVz/ry3I5zo4IJ_2BIobC/5nWwD7akwp5A/XzqLAJr21mH/cjfkiJFlq9y77G/1bzeLjs6zco1VtNrrz8EL/tJlbiHzqPNR1Mami/EAf48einPLf/Q.grow 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

Timestamp	kBytes transferred	Direction	Data
Jul 14, 2021 15:47:26.318327904 CEST	1351	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/grower/YjL_2BjDOrQaqruzKZl/J5qQT1PxhAWv_2ByqUpS3r/fw5c6vWOUvogF/fDf6v7zv/NA3IFZsX5L82cDak57at8n5/D4Cfgi7tVz/ry3I5zo4IJ_2BIobC/5nWwD7akwp5A/XzqLAJr21mH/cjfkiJFlq9y77G/1bzeLjs6zco1VtNrrz8EL/tJlbiHzqPNR1Mami/EAf48einPLf/Q.grow Server: Microsoft-IIS/10.0 request-id: e5b375e1-ab4a-b04b-d96a-87a09a6f4fed X-FEServer: MWHPR13CA0020 X-RequestId: 04dd39db-fffd-4c97-b71e-7102df85c47b X-Powered-By: ASP.NET X-FEServer: MWHPR13CA0020 Date: Wed, 14 Jul 2021 13:47:25 GMT Connection: close Content-Length: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5904 Parent PID: 5532

General

Start time:	15:46:03
Start date:	14/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\945.dll'
Imagebase:	0xf40000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.392687998.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.487967194.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.392901039.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.392858796.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.392613103.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.392808909.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.392529075.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.392768559.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.392386685.0000000002ED8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5780 Parent PID: 5904

General

Start time:	15:46:04
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\945.dll',#1
Imagebase:	0xbd0000
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 Show Windows behavior

Analysis Process: rundll32.exe PID: 5784 Parent PID: 5904

General

Start time:	15:46:04
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\945.dll,Clockcondition
Imagebase:	0xaf0000
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 | Show Windows behavior

Analysis Process: rundll32.exe PID: 5516 Parent PID: 5780

General

Start time:	15:46:04
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\945.dll',#1
Imagebase:	0xaf0000
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: 00000003.00000003.391393759.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.391313671.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.391228461.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.391141192.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.391066845.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.391440627.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.390980633.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.390863638.0000000004E68000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 1048 Parent PID: 5904

General

Start time:	15:46:09
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\945.dll,Dogwhen
Imagebase:	0xaf0000
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 | Show Windows behavior

Analysis Process: rundll32.exe PID: 1112 Parent PID: 5904

General

Start time:	15:46:13
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\945.dll,Sing
Imagebase:	0xaf0000
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

Show Windows behavior

Analysis Process: rundll32.exe PID: 1636 Parent PID: 5904

General

Start time:	15:46:19
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\945.dll,Wholegray
Imagebase:	0xaf0000
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

Show Windows behavior

Analysis Process: iexplore.exe PID: 6084 Parent PID: 792

General

Start time:	15:47:22
Start date:	14/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff64d950000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Copyright Joe Security LLC 2021

Analysis Process: iexplore.exe PID: 5208 Parent PID: 6084

General

Start time:	15:47:23
Start date:	14/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6084 CREDAT:17410 /prefetch:2
Imagebase:	0x13d0000
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

Show Windows behavior

Analysis Process: iexplore.exe PID: 3672 Parent PID: 6084

General

Start time:	15:47:25
Start date:	14/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6084 CREDAT:17414 /prefetch:2
Imagebase:	0x13d0000
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

Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021