



ID: 448651
Sample Name: 1c8.dll
Cookbook: default.jbs
Time: 15:45:17
Date: 14/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 1c8.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Rich Headers 15
Data Directories 15
Sections 15
Resources 15
Imports 15
Exports 15
Possible Origin 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 18
HTTP Packets 18
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19

Copyright Joe Security LLC 2021

Analysis Process: loaddll32.exe PID: 6956 Parent PID: 5972 19
General 19
File Activities 19
Analysis Process: cmd.exe PID: 6964 Parent PID: 6956 19
General 20
File Activities 20
Analysis Process: rundll32.exe PID: 6972 Parent PID: 6956 20
General 20
File Activities 20
Analysis Process: rundll32.exe PID: 6988 Parent PID: 6964 20
General 20
File Activities 21
Analysis Process: rundll32.exe PID: 7048 Parent PID: 6956 21
General 21
File Activities 21
Analysis Process: rundll32.exe PID: 7064 Parent PID: 6956 21
General 21
File Activities 22
Analysis Process: rundll32.exe PID: 7096 Parent PID: 6956 22
General 22
File Activities 22
Analysis Process: iexplore.exe PID: 5828 Parent PID: 800 22
General 22
File Activities 22
Registry Activities 22
Analysis Process: iexplore.exe PID: 2284 Parent PID: 5828 22
General 22
File Activities 23
Analysis Process: iexplore.exe PID: 6980 Parent PID: 5828 23
General 23
File Activities 23
Disassembly 23
Code Analysis 23

Copyright Joe Security LLC 2021

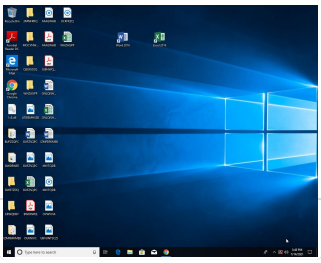
Windows Analysis Report 1c8.dll

Overview

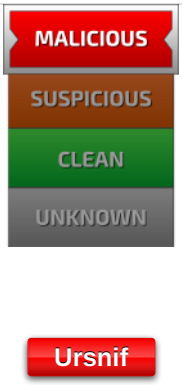
General Information

Sample Name:	1c8.dll
Analysis ID:	448651
MD5:	1c87b3ebc5ddf8f..
SHA1:	4579705a3e0e8b..
SHA256:	f2dfc3562e150ca..
Tags:	dll gozi
Infos:	

Most interesting Screenshot:



Detection

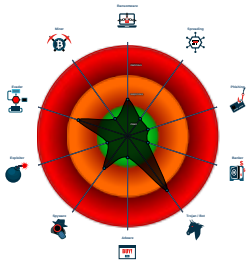


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 CPU …
- Contains functionality to query locale…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6956 cmdline: loaddll32.exe 'C:\Users\user\Desktop\1c8.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6964 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\1c8.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6988 cmdline: rundll32.exe 'C:\Users\user\Desktop\1c8.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6972 cmdline: rundll32.exe C:\Users\user\Desktop\1c8.dll,Clockcondition MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7048 cmdline: rundll32.exe C:\Users\user\Desktop\1c8.dll,Dogwhen MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7064 cmdline: rundll32.exe C:\Users\user\Desktop\1c8.dll,Sing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7096 cmdline: rundll32.exe C:\Users\user\Desktop\1c8.dll,Wholegray MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2284 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5828 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6980 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5828 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"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.849775483.0000000003618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.848756217.0000000004EB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.849876753.0000000003618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.850076693.0000000003618000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.848724837.0000000004EB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 15 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:



Yara detected Ursnif

Remote Access Functionality:

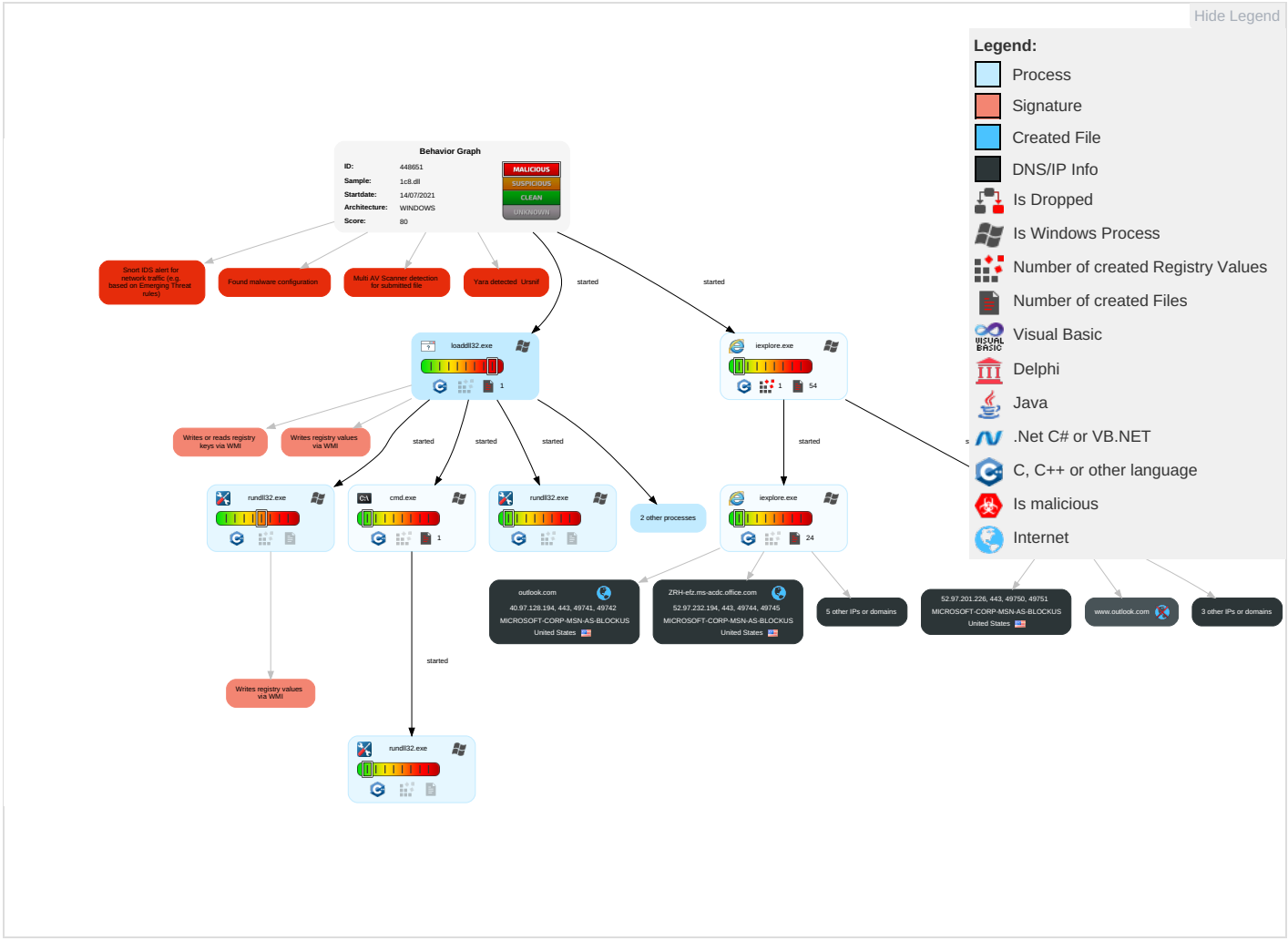


Yara detected Ursnif

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

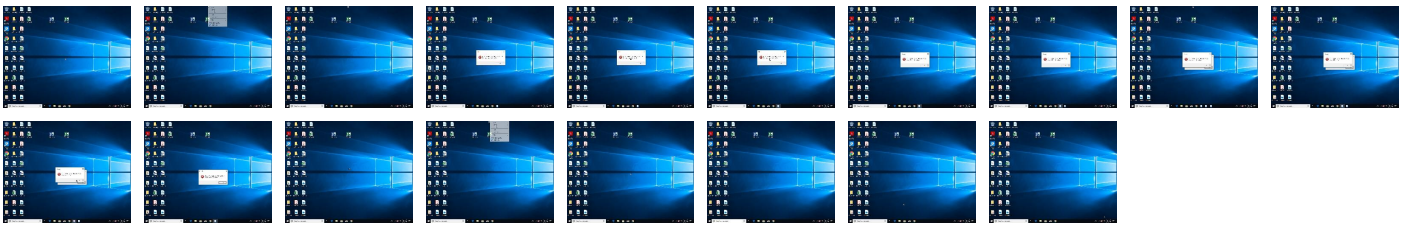
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1c8.dll	26%	Metadefender		Browse
1c8.dll	61%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.1170000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
6.2.rundll32.exe.4c20000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.8a0000.1.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
outlook.com	40.97.128.194	true	false		high
ZRH-efz.ms-acdc.office.com	52.97.232.194	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/grower/IGPiFOK9TunC/gPtC5_2F4YG/ZzNVH5SYgNPO4r/Psx6BaSL6yLcaujEgpw7P/tYMT5RnKSeCB9jBg/3iH6euhlA_2FGYG/rhrfnjjJUD3Y1TDXr8/g3m2c4nF8/bM6OTpEkWKHOq9wInEON/2HRIvyEq85fMK7VnDSk/ESY1C1z2RWNeT9llxDcxvu/GKJMCp_2FJD6L/hm1dCsQj.grow	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	448651
Start date:	14.07.2021
Start time:	15:45:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1c8.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:	24
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

Copyright Joe Security LLC 2021

Detection:	MAL
Classification:	mal80.troj.winDLL@18/7@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25% (good quality ratio 23.8%) • Quality average: 79.6% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 77% • 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
15:47:11	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
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%2FawF2z6INf5IJhbtrbLVkWA6i%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
outlook.com	uLTvM5APNY.exe	Get hash	malicious	Browse	• 40.93.207.0
	oEE058tCoG.exe	Get hash	malicious	Browse	• 40.93.207.1
	2Bmv1UZL2m.exe	Get hash	malicious	Browse	• 52.101.24.0
	oS4iWYYsx7.exe	Get hash	malicious	Browse	• 104.47.53.36
	P4SRvI1baM.exe	Get hash	malicious	Browse	• 104.47.54.36
	051y0i7M8q.exe	Get hash	malicious	Browse	• 40.93.207.0
	lEbR9gFgLr.exe	Get hash	malicious	Browse	• 104.47.54.36
	0OvBoFRzgC.exe	Get hash	malicious	Browse	• 104.47.54.36
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
	http://https://u4882271.ct.sendgrid.net/ls/click?upn=YFyCGXB2k7XEs51EAWvRp-2BQ6xaP5-2Bxv1vyI4slTyTp6VhtJSyiu7Ungt4CUf7KdGeEBPZ7lJ0WMtGrW3-2F8wXB5klqpkSCZwccYVceognA2U-3D57Rw_kfZ8cLppmcXDuIHKWdMrLPt30SkBa8ipQz83ljjYGp9c2flQixqYXWN470AqCFO8g1yhSwMHhN8-2BJK0vTLNC61PkTeWIrAs821yYsBfCbuclR33OfNLncv-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%2BAigE5ucTWat3Eej8US2xdckdOu0iDpwQIwMYKl9DLP2pKOIwIWa7isWu4stPeMJ%2BbSSC%2BrsVtg8U%2BWD1tF4Bc3%2FtEr3hJI4S3OomSDlwnU2PwUDgbmdkRVrT8Jiy8Xe4bfQ0dyp5k2o%2Bf2eztEQzNsZlKz0xjWSRZcdjYCg9vWmNNNSvSwsWNybr8UBeONKYmj4PdCOwhNBWdvur%2BK4Wx1bqcPE26q7z8kpyQ4hJ2vOCvXmdlnZ37w0%2BAGvM3H2V03OaxIsBHrlCuyiPhQWq8qdKOB4lg1EmFibK759dnK%2FawF2z6INf5lJhbtrbLVkWA6i%2FuckBPOJvVXHWYj5SHhB8X%2FZz	Get hash	malicious	Browse	• 52.97.232.194
	okayfreedomwr.exe	Get hash	malicious	Browse	• 52.97.232.194

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
	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
	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.{0A0F511A-E4AA-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.0059703311922683
Encrypted:	false
SSDEEP:	192:rkZn7ZG2JW0t/iffeszMQkB8kDid6coDE7uMsJE7tdELfV9ELtmDqpLmT0DupJFj:rUt94gY2pXkk8KHOohz
MD5:	F57C97FB7BBD362FE7E7673DE3468F0B
SHA1:	EB35668061617D36F4898660556685F9BB53D2F8
SHA-256:	4AC85D49BC0D65C1620CB0619CE51A99BBBAFA0C845F1C412601F01C95EBD46C
SHA-512:	6E0327CC091324432B94A36F33CB36C6F1C368F57E0A36B33CFF14B298907600F5946DC417257703829B2F6F5DF6FC29AF7D5E2EDDD5ADDB61E1911E2A35EA3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0A0F511A-E4AA-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0A0F511C-E4AA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.8457791105103485
Encrypted:	false
SSDEEP:	96:rVZy7Qm6SHBSJjx/21WxkMOi1Bp3+Lx1Bp3+opnA:rVZy7Qm6IkJjB21WGMOi1/0x1/PnA
MD5:	174169A2DC47832FAF2D867313A7C955
SHA1:	5D5DA7C142D63F87ADE749CD6B9B71D9CE561159
SHA-256:	DF8991E3F284A5855966524342CEFB94168D3B8E9AD26E231D61F1F0E24B9E3C
SHA-512:	2ED28D5A98E88DDA7A7583F34370126CDDBDA187443956F7BF2B6AADF8B5FA1AC00C1B2DC5988DEE0B83ED190DCC3C96AF546DA2571DB1F905744D2E3C5F9 D4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0A0F511E-E4AA-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27448
Entropy (8bit):	1.8711021214705452
Encrypted:	false
SSDEEP:	96:rkZzQ36dHBSljF/2ZWxkM6yXB5Ct9RXB5CtgIpA:rkZzQ365klj12ZWGM6yXPCPRXPCLpA
MD5:	BAA7A8C3820B42D05B560B1293167402
SHA1:	3A5C8319E1A650DA9E3826B1CB003B5D4E14C3EA
SHA-256:	8B485DF077C5DC61A02CFFEFE161BA5F97C2F0BD01630E25B90F34A5B57E2ECC
SHA-512:	0762D2547F2B9C71E91CA1628821A6B175931270248E70F35B27B2B262C8201B3944B2D00848A2A5F017A05ABB96D7DBFACD07109638D54287D01438F5BB7A09
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:	modified
Size (bytes):	89
Entropy (8bit):	4.575366195605629
Encrypted:	false
SSDEEP:	3:oVXUtJf0fSIqH8JOGXnEtJf0fSIZun:o9UtJbHqEtJWu
MD5:	8014349F0CD85213AF05E13A1C7A28BA
SHA1:	9B76E3C05F7F406A1876A7121B0E967F9ECC7999
SHA-256:	3D75FBDB39C630D2674A606AB448B0DA5491644665965555325 5B395A63EF7C9
SHA-512:	00BFD8F50455E2B595693C0EDFDA2107AF7CC296819D7C5BF68F1AE0D6621D7017AE0C22A8B4BE0BDBE60F7EFEEA84CA82AC77E49570DAC0ED08FF6606D03 9B
Malicious:	false
Preview:	[2021/07/14 15:47:36.558] Latest deploy version: ..[2021/07/14 15:47:36.558] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF34CE60BF8360E948.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5990802949288698
Encrypted:	false

C:\Users\user\AppData\Local\Temp\~DF34CE60BF8360E948.TMP	
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo5S9lo5C9lW5jdSodkrbkrRIZpIdkrRllfll4opI3:kBqoITFw4yt3y+c
MD5:	CF1187ECDBD8B9908C9095F68448FA82
SHA1:	C4F49BABEF42F0DE41A9A8D192089BD294E85D14
SHA-256:	9BA9D7F60EF1BB59B86E61C97F7AE74EB2A3321F74A3BB2AFF63374E0C445878
SHA-512:	5E84D9401E3A339E83244E9B57D971996078AC24035720EC19AA7B64315A057CB7C2A5E4E31BB1D7668D1AB7CCDA3108D6B5E38F98D149056D606E97FCBB534
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

General

SHA256:	f2dfc3562e150ca045557559269c3c21531bb8529286410 9fd2ceca4fe0f1ea9
SHA512:	0a1e8a5afd02216b2b0f08c9c8b5866938c6c66bdc90250 1aeb2b0dc4a19da7b1018865b4c99628655507a545f507 e2aa53d74b0e68f0fd55c979a285a46e026
SSDEEP:	6144:vC8nRa6tXFOspzA7z6NZVeC8i795fubASK9beZT X3l8Eo:J0SVOsp5VWi7PWoBeZTX36
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	0.619812588611	data	6.63194567015	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
07/14/21-15:47:37.828655	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49741	80	192.168.2.4	40.97.128.194

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 14, 2021 15:47:37.643353939 CEST	192.168.2.4	8.8.8.8	0xbf05	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.444652081 CEST	192.168.2.4	8.8.8.8	0xa503	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.572945118 CEST	192.168.2.4	8.8.8.8	0xc891	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.905317068 CEST	192.168.2.4	8.8.8.8	0xd6a8	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.384074926 CEST	192.168.2.4	8.8.8.8	0x3e91	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.462891102 CEST	192.168.2.4	8.8.8.8	0x9459	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
Jul 14, 2021 15:47:37.656598091 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:37.656598091 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:37.656598091 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:37.656598091 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:37.656598091 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:37.656598091 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:37.656598091 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 14, 2021 15:47:37.656598091 CEST	8.8.8.8	192.168.2.4	0xbf05	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.457087994 CEST	8.8.8.8	192.168.2.4	0xa503	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:38.457087994 CEST	8.8.8.8	192.168.2.4	0xa503	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:38.457087994 CEST	8.8.8.8	192.168.2.4	0xa503	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:38.457087994 CEST	8.8.8.8	192.168.2.4	0xa503	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:38.457087994 CEST	8.8.8.8	192.168.2.4	0xa503	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.194	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.457087994 CEST	8.8.8.8	192.168.2.4	0xa503	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.186.114	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.457087994 CEST	8.8.8.8	192.168.2.4	0xa503	No error (0)	ZRH-efz.ms-acdc.office.com		52.98.163.18	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.457087994 CEST	8.8.8.8	192.168.2.4	0xa503	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.585489035 CEST	8.8.8.8	192.168.2.4	0xc891	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:38.585489035 CEST	8.8.8.8	192.168.2.4	0xc891	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:38.585489035 CEST	8.8.8.8	192.168.2.4	0xc891	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:38.585489035 CEST	8.8.8.8	192.168.2.4	0xc891	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.585489035 CEST	8.8.8.8	192.168.2.4	0xc891	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.186.114	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.585489035 CEST	8.8.8.8	192.168.2.4	0xc891	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.585489035 CEST	8.8.8.8	192.168.2.4	0xc891	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.226	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.917916059 CEST	8.8.8.8	192.168.2.4	0xd6a8	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.917916059 CEST	8.8.8.8	192.168.2.4	0xd6a8	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.917916059 CEST	8.8.8.8	192.168.2.4	0xd6a8	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.917916059 CEST	8.8.8.8	192.168.2.4	0xd6a8	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.917916059 CEST	8.8.8.8	192.168.2.4	0xd6a8	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.917916059 CEST	8.8.8.8	192.168.2.4	0xd6a8	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.917916059 CEST	8.8.8.8	192.168.2.4	0xd6a8	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:38.917916059 CEST	8.8.8.8	192.168.2.4	0xd6a8	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.397406101 CEST	8.8.8.8	192.168.2.4	0x3e91	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:39.397406101 CEST	8.8.8.8	192.168.2.4	0x3e91	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 14, 2021 15:47:39.397406101 CEST	8.8.8.8	192.168.2.4	0x3e91	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:39.397406101 CEST	8.8.8.8	192.168.2.4	0x3e91	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:39.397406101 CEST	8.8.8.8	192.168.2.4	0x3e91	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.226	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.397406101 CEST	8.8.8.8	192.168.2.4	0x3e91	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.186.114	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.397406101 CEST	8.8.8.8	192.168.2.4	0x3e91	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.397406101 CEST	8.8.8.8	192.168.2.4	0x3e91	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.242	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.477440119 CEST	8.8.8.8	192.168.2.4	0x9459	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:39.477440119 CEST	8.8.8.8	192.168.2.4	0x9459	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:39.477440119 CEST	8.8.8.8	192.168.2.4	0x9459	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 14, 2021 15:47:39.477440119 CEST	8.8.8.8	192.168.2.4	0x9459	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.194	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.477440119 CEST	8.8.8.8	192.168.2.4	0x9459	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.242	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.477440119 CEST	8.8.8.8	192.168.2.4	0x9459	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.210	A (IP address)	IN (0x0001)
Jul 14, 2021 15:47:39.477440119 CEST	8.8.8.8	192.168.2.4	0x9459	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.194	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	192.168.2.4	49741	40.97.128.194	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 14, 2021 15:47:37.828655005 CEST	1088	OUT	GET /grower/IGPiFOK9TunC/gPtC5_2F4YG/ZzNVH5SYgNPO4r/Psx6BaSL6yLcaujEgpw7P/tYMT5RnKSeCB9jBg/3iH6euhlA_2FGYG/rhrfnjjJUD3Y1TDXr8/g3m2c4nF8/bM6OTpEkWKHOq9wInEON/2HRIvyEq85fMK7VnDSk/ESY1C1z2RWNeT9llxDcxvu/GKJMCp_2FJD6L/hm1dCsQj.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
Jul 14, 2021 15:47:37.960118055 CEST	1089	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/grower/IGPiFOK9TunC/gPtC5_2F4YG/ZzNVH5SYgNPO4r/Psx6BaSL6yLcaujEgpw7P/tYMT5RnKSeCB9jBg/3iH6euhlA_2FGYG/rhrfnjjJUD3Y1TDXr8/g3m2c4nF8/bM6OTpEkWKHOq9wInEON/2HRIvyEq85fMK7VnDSk/ESY1C1z2RWNeT9llxDcxvu/GKJMCp_2FJD6L/hm1dCsQj.grow Server: Microsoft-IIS/10.0 request-id: cdb1ff5c-81d3-c2f3-3e0b-91fae0e5d451 X-FEServer: DM5PR2201CA0006 X-RequestId: 7db06cb8-a172-45d8-9669-20c12b4c4bcd X-Powered-By: ASP.NET X-FEServer: DM5PR2201CA0006 Date: Wed, 14 Jul 2021 13:47:36 GMT Connection: close Content-Length: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6956 Parent PID: 5972

General

Start time:	15:46:06
Start date:	14/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\1c8.dll'
Imagebase:	0x1190000
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: 00000000.00000003.849775483.0000000003618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.849876753.0000000003618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.850076693.0000000003618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.850098978.0000000003618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.850034271.0000000003618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.849999289.0000000003618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.918801492.0000000003618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.849834165.0000000003618000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.849965613.0000000003618000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6964 Parent PID: 6956

General

Start time:	15:46:06
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\1c8.dll',#1
Imagebase:	0x11d0000
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: 6972 Parent PID: 6956

General

Start time:	15:46:06
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\1c8.dll,Clockcondition
Imagebase:	0x10f0000
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: 6988 Parent PID: 6964

General

Start time:	15:46:06
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\1c8.dll',#1
Imagebase:	0x10f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000003.00000003.848756217.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.848724837.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.848569421.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.848820548.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.919640780.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.848847828.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.848790447.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.848684716.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.848623660.0000000004EB8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7048 Parent PID: 6956

General

Start time:	15:46:11
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\1c8.dll,Dogwhen
Imagebase:	0x10f0000
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: 7064 Parent PID: 6956

General

Start time:	15:46:15
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\1c8.dll,Sing
Imagebase:	0x10f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 7096 Parent PID: 6956

General

Start time:	15:46:20
Start date:	14/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\1c8.dll,Wholegray
Imagebase:	0x10f0000
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: 5828 Parent PID: 800

General

Start time:	15:47:32
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:	0x7ff7704e0000
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

Analysis Process: iexplore.exe PID: 2284 Parent PID: 5828

General

Start time:	15:47:35
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:5828 CREDAT:17410 /prefetch:2
Imagebase:	0x8f0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6980 Parent PID: 5828

General

Start time:	15:47:37
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:5828 CREDAT:17414 /prefetch:2
Imagebase:	0x8f0000
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