ID: 444548
Sample Name:
60e40fb428612.dll
Cookbook: default.jbs
Time: 10:12:25
Date: 06/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

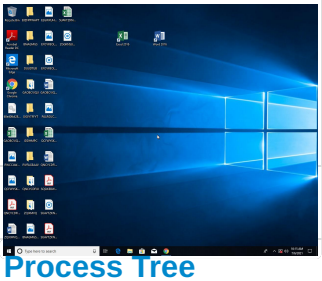
Windows Analysis Report 60e40fb428612.dll

Overview

General Information

Sample Name:	60e40fb428612.dll
Analysis ID:	444548
MD5:	c6bfea479b46b9e.
SHA1:	c7f449ab51a4779.
SHA256:	62dbfe723197430.
Tags:	dll enel geo gozi isfb ita ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

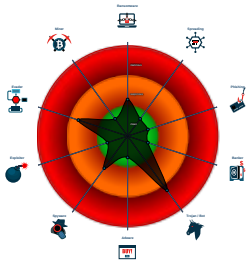
Ursnif

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Contains functionality which may be…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6680 cmdline: loaddll32.exe 'C:\Users\user\Desktop\60e40fb428612.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6708 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\60e40fb428612.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6760 cmdline: rundll32.exe 'C:\Users\user\Desktop\60e40fb428612.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6748 cmdline: rundll32.exe C:\Users\user\Desktop\60e40fb428612.dll,Clockcondition MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6792 cmdline: rundll32.exe C:\Users\user\Desktop\60e40fb428612.dll,Dogwhen MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6804 cmdline: rundll32.exe C:\Users\user\Desktop\60e40fb428612.dll,Sing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6816 cmdline: rundll32.exe C:\Users\user\Desktop\60e40fb428612.dll,Wholegray MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6312 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1320 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6312 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 3176 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"ovNAU+HRorLZmwnDvbYFDY7UA+FTIAnF2uJSQd0M+N3ep6CVEhoDrEXACstP09QHK7cBl9nMAaFI1as0K4aXOQKngdScIQbDa3MQ98Ce9MYRMvxGUI05fSIRRFzMYffOXQr97vVUUUPjsYgfkDWS2eKPxSe5dz/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
00000004.00000003.375971100.00000000053D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.375934102.00000000053D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.375882980.00000000053D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.375768564.00000000053D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.375954554.00000000053D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

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 registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

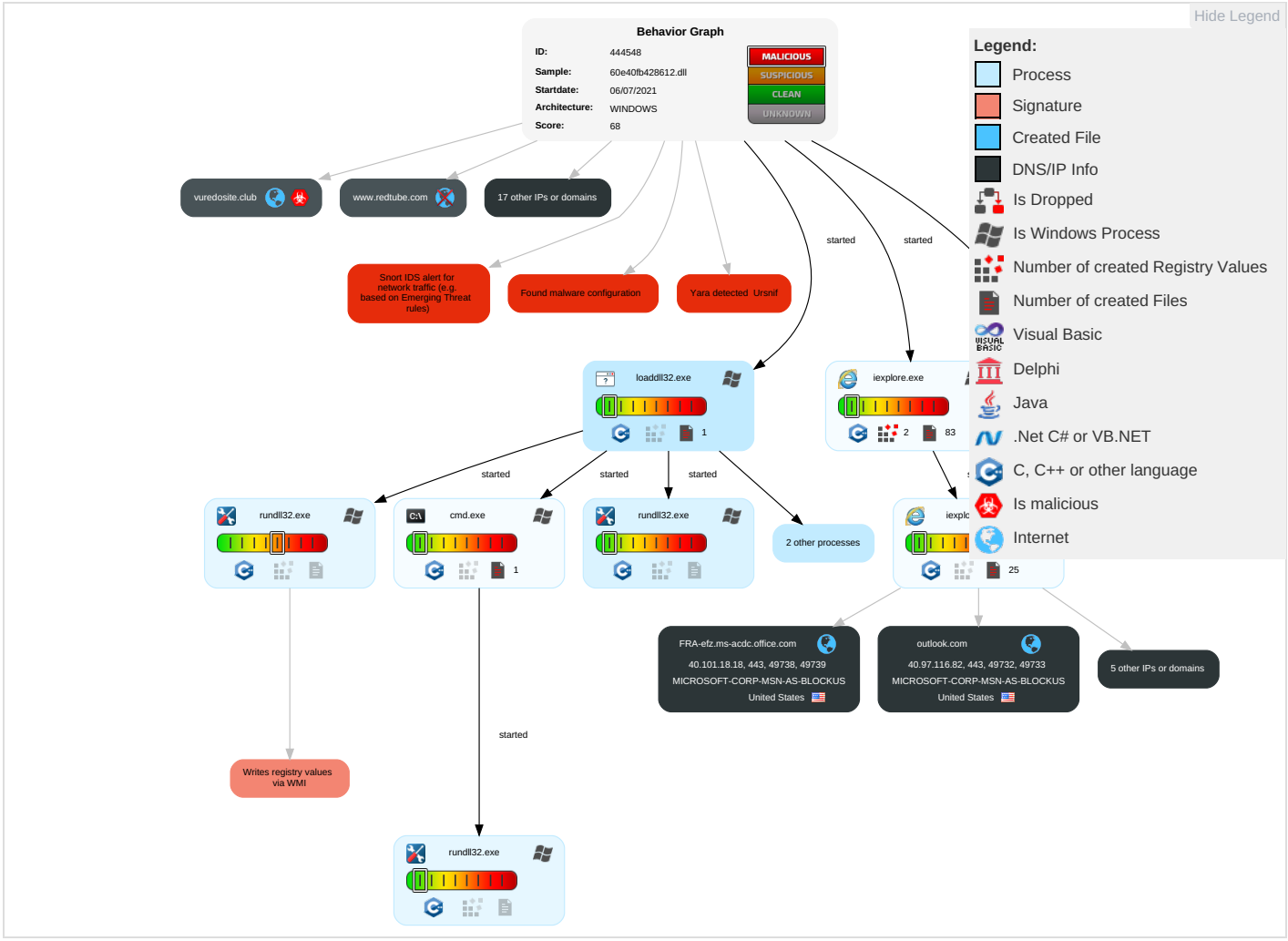
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 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 1	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	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.2ba0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.c20000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
vip0x055.ssl.rncdn5.com	0%	Virustotal		Browse
cs733.wpc.rncdn4.com	0%	Virustotal		Browse
vip0x04f.ssl.rncdn5.com	0%	Virustotal		Browse
ei.rdtcdn.com.sds.rncdn7.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.de	142.250.201.195	true	false		high
stats.l.doubleclick.net	142.250.102.155	true	false		high
redtube.com	66.254.114.238	true	false		high
vip0x055.ssl.rncdn5.com	205.185.208.85	true	false	• 0%, Virustotal, Browse	unknown
cs733.wpc.rncdn4.com	192.229.221.206	true	false	• 0%, Virustotal, Browse	unknown
HHN-efz.ms-acdc.office.com	52.97.201.18	true	false		high
vip0x04f.ssl.rncdn5.com	205.185.208.79	true	false	• 0%, Virustotal, Browse	unknown
hubtraffic.com	66.254.114.32	true	false		high
outlook.com	40.97.116.82	true	false		high
ei.rdtcdn.com.sds.rncdn7.com	64.210.135.68	true	false	• 0%, Virustotal, Browse	unknown
ads.trafficjunky.net	66.254.114.38	true	false		high
vuredosite.club	37.120.222.6	true	true		unknown
FRA-efz.ms-acdc.office.com	40.101.18.18	true	false		high
vip0x08e.ssl.rncdn5.com	205.185.208.142	true	false		unknown
static.trafficjunky.com	unknown	unknown	false		high
www.redtube.com	unknown	unknown	false		high
ci-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

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	444548
Start date:	06.07.2021
Start time:	10:12:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	60e40fb428612.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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.troj.winDLL@17/14@17/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.7% (good quality ratio 17.9%) • Quality average: 79.9% • Quality standard deviation: 28%
HCA Information:	• Successful, ratio: 58% • 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
10:14:14	API Interceptor	1x Sleep call for process: rundll32.exe modified
10:14:24	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
40.101.18.18	PURCHASE ORDER#34556558.exe	Get hash	malicious	Browse	
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	
	SS21 order IN644.exe	Get hash	malicious	Browse	
	http://https://sammsung055.z13.web.core.windows.net/#sandra.leung@bms.com	Get hash	malicious	Browse	
	http://https://techingcode22.z19.web.core.windows.net/#christoph.metzger@dufry.ch	Get hash	malicious	Browse	
	Payment_Remittance_Copy_pdf.html	Get hash	malicious	Browse	
	http://https://normal777.z19.web.core.windows.net/#joao.dias@novobanco.pt	Get hash	malicious	Browse	
	http://https://conectivait.com/t3med/proposal	Get hash	malicious	Browse	
	http://blog.ploytrip.com/z9cr/Pages/UxiQIlomnGiGKODewvEaBYLyCJh/	Get hash	malicious	Browse	
	http://https://sap-my.sharepoint.com/:f:/p/matthew_shaw/Ehpzmgu3VfZAsMu8vLvBrCQBHVyLMMbSpZvaMqHdiTvV9A?e=QO7ALe	Get hash	malicious	Browse	
40.97.116.82	zHUScMPOlZ.dll	Get hash	malicious	Browse	
	nT5pUwoJSS.dll	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	82attachmen.exe	Get hash	malicious	Browse	
	62lette.exe	Get hash	malicious	Browse	
	5transcrip.exe	Get hash	malicious	Browse	
	1message.exe	Get hash	malicious	Browse	
	49instructio.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	52DOCUMEN.exe	Get hash	malicious	Browse	
	25messag.exe	Get hash	malicious	Browse	
	fuck.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
stats.l.doubleclick.net	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
	Sleek_Free.exe	Get hash	malicious	Browse	• 74.125.140.155
www.google.de	vNiyRd4GcH.exe	Get hash	malicious	Browse	• 142.250.186.35
	DocuSign-June-SOA-Dues.261.htm	Get hash	malicious	Browse	• 142.250.184.227
	XqnM8G36Ih.exe	Get hash	malicious	Browse	• 142.250.184.195

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bmaphis@cardinaltek.com_16465506 AMDocAtt.HTML	Get hash	malicious	Browse	• 142.250.184.195
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 142.250.184.195
	HRXoZLG4ym.exe	Get hash	malicious	Browse	• 142.250.184.195
	Hngx5CdG2D.exe	Get hash	malicious	Browse	• 142.250.181.227
	muestra6999.exe	Get hash	malicious	Browse	• 142.250.181.227
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 172.217.16.99
	crt9O3URua.exe	Get hash	malicious	Browse	• 172.217.16.99
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 172.217.16.99
	Ref#Doc30504871 Wyg.htm	Get hash	malicious	Browse	• 172.217.16.99
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 216.58.207.131
	Sleek_Free.exe	Get hash	malicious	Browse	• 216.58.207.131
	wzdu53.exe	Get hash	malicious	Browse	• 216.58.207.131
	teX5sUCWAg.exe	Get hash	malicious	Browse	• 142.251.36.227
	teX5sUCWAg.exe	Get hash	malicious	Browse	• 142.251.36.227
	SetupFA.exe	Get hash	malicious	Browse	• 172.217.20.3
	aydrxnitvo.exe	Get hash	malicious	Browse	• 172.217.23.67
	sP2AXSWC73.exe	Get hash	malicious	Browse	• 172.217.16.99

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	9cYXsscTTT.exe	Get hash	malicious	Browse	• 104.42.151.234
	TestTakerSBBrowser.exe	Get hash	malicious	Browse	• 137.117.66.167
	mJSDCeNxFi.exe	Get hash	malicious	Browse	• 40.88.32.150
	oEE058tCoG.exe	Get hash	malicious	Browse	• 40.93.212.0
	zHUScMPOlZ.dll	Get hash	malicious	Browse	• 40.97.116.82
	hsIF8b0YX1.msi	Get hash	malicious	Browse	• 191.235.71.131
	x86_x64_setup.exe	Get hash	malicious	Browse	• 104.43.193.48
	h3hlbLDpl8.exe	Get hash	malicious	Browse	• 13.64.90.137
	PAYMENT.HTML	Get hash	malicious	Browse	• 13.71.84.154
	JOB-in.line e.K.- Purchase Order 19600396 & 19600397.xlsx.exe	Get hash	malicious	Browse	• 13.82.24.228
	y3sBoQe6u7.exe	Get hash	malicious	Browse	• 52.170.189.162
	NC46O8xw5Z.exe	Get hash	malicious	Browse	• 52.170.189.162
	input.06.21.doc	Get hash	malicious	Browse	• 52.109.32.41
	PaymentConfirmation.pdf.exe	Get hash	malicious	Browse	• 13.90.75.180
	iaxfO8uzGB.exe	Get hash	malicious	Browse	• 20.184.2.45
	lumion.pro.v11-cgp-tpc.exe	Get hash	malicious	Browse	• 52.142.114.176
	ContactocelqnxthGOOwgjC%mu_NtgaG3(76852891932Contacto.bat	Get hash	malicious	Browse	• 52.167.55.56
	kvA3VL7NNB.exe	Get hash	malicious	Browse	• 40.118.53.192
	Tkl2kVaz5o.exe	Get hash	malicious	Browse	• 13.82.24.228
	Gnqavfhmcsecxlwdiltkkverstraextmrm.exe	Get hash	malicious	Browse	• 20.98.18.253
MICROSOFT-CORP-MSN-AS-BLOCKUS	9cYXsscTTT.exe	Get hash	malicious	Browse	• 104.42.151.234
	TestTakerSBBrowser.exe	Get hash	malicious	Browse	• 137.117.66.167
	mJSDCeNxFi.exe	Get hash	malicious	Browse	• 40.88.32.150
	oEE058tCoG.exe	Get hash	malicious	Browse	• 40.93.212.0
	zHUScMPOlZ.dll	Get hash	malicious	Browse	• 40.97.116.82
	hsIF8b0YX1.msi	Get hash	malicious	Browse	• 191.235.71.131
	x86_x64_setup.exe	Get hash	malicious	Browse	• 104.43.193.48
	h3hlbLDpl8.exe	Get hash	malicious	Browse	• 13.64.90.137
	PAYMENT.HTML	Get hash	malicious	Browse	• 13.71.84.154
	JOB-in.line e.K.- Purchase Order 19600396 & 19600397.xlsx.exe	Get hash	malicious	Browse	• 13.82.24.228
	y3sBoQe6u7.exe	Get hash	malicious	Browse	• 52.170.189.162
	NC46O8xw5Z.exe	Get hash	malicious	Browse	• 52.170.189.162
	input.06.21.doc	Get hash	malicious	Browse	• 52.109.32.41
	PaymentConfirmation.pdf.exe	Get hash	malicious	Browse	• 13.90.75.180
	iaxfO8uzGB.exe	Get hash	malicious	Browse	• 20.184.2.45
	lumion.pro.v11-cgp-tpc.exe	Get hash	malicious	Browse	• 52.142.114.176

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ContactocelqnxthGOOwgjC%mu_NtgaG3(76852891932Contacto.bat	Get hash	malicious	Browse	• 52.167.55.56
	kvA3VL7NNB.exe	Get hash	malicious	Browse	• 40.118.53.192
	Tkl2kVaz5o.exe	Get hash	malicious	Browse	• 13.82.24.228
	Gnqavfhmcsecxlwdiltkkverstraextmrm.exe	Get hash	malicious	Browse	• 20.98.18.253

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9F4ECD44-DE7D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.772924635523489
Encrypted:	false
SSDEEP:	96:rIZDZ+21jWaQOtaQkjNfaQkJjJb1MaPJWxTTm+PJqDB:rIZDZ+21jWpOtpmfpaxMrvcB
MD5:	7C8C1828F92E6CBAE509B37492922C2B
SHA1:	5EE8D6D94E12F48FAD9A2525022E45FAF0AED6F3
SHA-256:	78DE3376B09D44F1856E233DB1AAC58F16694D92B0F583A2D688F8B60CA5E7F6
SHA-512:	81E018F7A9615498834CACCDABD80C27263253BA0C716791E9359D4E1760C4DE3676C30441957934EF73242FD73CB55F1EB10BBC660C6D4DC7F43604C26DCB9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9F4ECD46-DE7D-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27440
Entropy (8bit):	1.8685329661065735
Encrypted:	false
SSDEEP:	192:rsZXQ765kIbjh2ISWZMJ6QMcm85DxxQMcm85DLcm81A:rsA+KIHQIRik2NP2NIW
MD5:	A8283B1F89E8FE3D9516A5879CF22529
SHA1:	0C0D464DC572D4DFE01E8A61A40AD2D7A169F2F3
SHA-256:	5A4DB801F0CFC7D341D131116E6694AD8DB16C00B0FB9EB9B3323998F79ED86F
SHA-512:	553912B4860BE810CC086F9F54BD6F92009533A259005E38E555FD60DD01AC4AF16BC70F8787CFD7A1959831A4CBCE33B32FDC82AB563B40729AD47F6054D3A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.1370133199807855
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE+loYlow4nWimI002EtM3MHdNMNxOE+loYlow4nWimI00ObVbkEtMb:2d6NxOnoMoJSZHKd6NxOnoMoJSZ76b
MD5:	8CDDF656C19A8FE75BE2FB5242BECF8B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
SHA1:	8AF0738E35451565919735590D77CDA9BC9D5877
SHA-256:	01FCEF5F8E8210E98053200C15DCC267A37915731B47B8476229C0A7D8963018
SHA-512:	ABF67CAFAE3E2C57487997A125950BE678740F41BBE1D77114EDA032CDDBAB75CB508E1687AC5326BEF4E4F15B577CED840B14DCD8493730ECD36F733CD7FA 8B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x75b61584,0x01d7728a</date> accdate>0x75b61584,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x75b61584,0x01d7728a</date><accdate>0 x75b61584,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.141239430132834
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k2E4Ew4nWimI002EtM3MHdNMNxe2k2Esw4nWimI00Obkak6EtMb:2d6Nxr8TJSZHKd6Nxr8sJSZ7Aa7b
MD5:	C18FB96A2677A8AD21264174E9B5D06C
SHA1:	144F2CE5723B6062136BD6A688C103FCDD1381E1
SHA-256:	58D3BC4C56E6C3CE9CFB2B854D7939E4BEA51E6473A0FEC1E2F1DDE9B3473039
SHA-512:	E307AB54B10810092B08E2B883020339B71C4122C5B14225E7CCB02A934C695EF756DE71CDCE529AFAE6129455005A1B6074BD8227199AC5F1C52141BE832C91
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x75a6d344,0x01d7728a</date><a ccdate>0x75a6d344,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x75a6d344,0x01d7728a</date><a ccdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.155771814519474
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL+loYlow4nWimI002EtM3MHdNMNxvL+loYlow4nWimI00ObmZEtMb:2d6NxveoMoJSZHKd6NxveoMoJSZ7mb
MD5:	10E1BB06FA11954027983BE655C1DE90
SHA1:	CD0EB6F6E72AD63AF7564AE8186D05329BC3910D
SHA-256:	5CDD7685923D3845E70F06DA25FC27423CF7A16BA753A325B09E5B565227A41B
SHA-512:	4794D67ADE225AB3CF101428475CBF2D5959A018931274FDD9393B51F5AB664DE906F41D9F9A344DCAE472F58B7CCDBD4435B47306057B3FCDF4FCDAC9C39C 0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x75b61584,0x01d7728a</date> <accdate>0x75b61584,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>.. <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x75b61584,0x01d7728a</date><accda te>0x75b61584,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.126076628714451
Encrypted:	false
SSDEEP:	12:TMHdNMNxiysw4nWimI002EtM3MHdNMNxiysw4nWimI00Obd5EtMb:2d6NxFsJSZHKd6NxFsJSZ7Jjb
MD5:	67F23DD4BD5B4AC91CDEB4AD19EF1383
SHA1:	D9BEDAA2208FAFC9A2028F1A019B85C598DB1225
SHA-256:	F95BDD163A8A27AAD36E89BC3EEEADFE2FC4B4477BAE1874D3A7821220D6BA83
SHA-512:	66BC54AECD9BD78AC57A43E6FE848A7BA83A86E7C02ACE825AF06BFEAC42932740C520E073588A5F087E661488B1CB3B98896D021AA3DEB785E1FD004F8DFA DB
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x75ae7464,0x01d7728a</date><acc date>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.168113819529659
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw+loYlow4nWimI002EtM3MHdNMNxhGw+loYlow4nWimI00Ob8K075t:2d6NxQzoMoJSZHKd6NxQzoMoJSZ7YKa/
MD5:	BC732ADD8E3E3417EAA611F9E7FCCF9D
SHA1:	D572BA10272A9099184EA2FF1CD59A3054B11E66
SHA-256:	6F218251411D737BCEB92E403637ACE6859C4868659EB7EB34BED735A0C9722A
SHA-512:	AD7ABC77A5BC674E4B083C0F95D8C45AB4D75086CF0B430C0ECCBDD8237328DCFD373FD2B3F341D2E5BBCBDF4DE9B1D1AF2385D1A97A65ADB86CDA7D8BE94AD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x75b61584,0x01d7728a</date><accdate>0x75b61584,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x75b61584,0x01d7728a</date><accdate>0x75b61584,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.122691731433799
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nysw4nWimI002EtM3MHdNMNx0nyYlow4nWimI00ObxEtMb:2d6Nx0ysJSZHKd6Nx0yMoJSZ7nb
MD5:	9373F79A947760C9CEFCA656E1A755AA
SHA1:	AEAE50D2928951B78741F9629C58E595D2C18DFB
SHA-256:	FDF2AF93747CCD74C4FD3BEA2B4D8D4109D2FAA33DC5786359B562DE27F2E9B6
SHA-512:	72A0FBA2E8FE19B731DB087C509B0F3F17C43EED6B83144C1C1BDC8F61AD9A04E4815217DA766062E465BF3A91600365123636DA44D359422BF22E90D999D368
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75b61584,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.150522085625073
Encrypted:	false
SSDEEP:	12:TMHdNMNxxysw4nWimI002EtM3MHdNMNxxysw4nWimI00Ob6Kq5EtMb:2d6NxwsJSZHKd6NxwsJSZ7ob
MD5:	1B603D219A9EE1A601FB90A6F99E3020
SHA1:	6AF87033C2BF262B43C2BD788BC0E5ECD4A51538
SHA-256:	E957E32B11A1A3628E389262FDAC37F676D93C7BA1CE1A260713C802FDDEC00B
SHA-512:	70938D2AEEFCD35F830D70F7A7ACE4640EE3204202500082363D4B5D523F4AAF58CAFCEE57FBAFF4D73D1C6630D5DC18DBB57BF393C2ADE360F44359F9B092D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.130028839755316
Encrypted:	false
SSDEEP:	12:TMHdNMNxcysw4nWimI002EtM3MHdNMNxcysw4nWimI00ObVEtMb:2d6NxTsJSZHKd6NxTsJSZ7Db
MD5:	8C15E261BD350519B068797A0AA6B0A1
SHA1:	58E8845D8BEE59243E2D9A7439709CE82B795C90
SHA-256:	4F4289FB852430851C279E6B212F03DE22111AE236328CAEFFDE46C12F9CBB37
SHA-512:	7FD2535AB0EB34DEE45430B653BD362D7C3D2BDD7EB8178FD71D1B3E9EEB55E1D412AEF45CF1F61A9E398A015535143FB7BAF581C004F78448ACD321A5F39A79
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.111602801743394
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnysw4nWimI002EtM3MHdNMNxfnysw4nWimI00Obe5EtMb:2d6NxasJSZHKd6NxasJSZ7ijb
MD5:	095286053DFE08A9048F59187130C671
SHA1:	EC18C9E731C770057A3E9AB28EBD0BF65646E9A5
SHA-256:	10753B1D07A0270419982E614D34B5F1B3EEDE2F10C4F9498CF39B8AAF492368
SHA-512:	5A7373872D50AE0395FF1DCEC8245FFF1BB61248BE4846705BB24EB880EF9D42C391E4ACFD84FF57DAFC4199F0A53193A858FFA6D99801A7B44C85E5B8E8528
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x75ae7464,0x01d7728a</date><accdate>0x75ae7464,0x01d7728a</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

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):	4.456558184868483
Encrypted:	false
SSDEEP:	3:oVXUoHFQ4ImW8JOGXnEoHFQ4mn:o9UolQdHqEolQB
MD5:	91D290BAECADD68327326320765FA8AC
SHA1:	EF4BE826977032F459D30059B9E511A73A8D0168
SHA-256:	DC9A8FE16024DB2B0FCEF83F274A9482FFFBCFD023D459155159000CE616693C
SHA-512:	3DCE051F08D5FEA0318A60276EF2C275D5009067CCCF0F0A82644B023D68766A925DA1490C77E4E014EE3DA016BA503BA02177265C5C3CEEDFDA5E7666C7045
Malicious:	false
Preview:	[2021/07/06 10:14:31.195] Latest deploy version: ..[2021/07/06 10:14:31.195] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF1C465EC4A4AE6446.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4123024469502063
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loxF9loT9lW6Q2jW:kBqoIUK6Q2jW
MD5:	ECC7DD9AEB22ED33DC2B310B6B0F9A4D
SHA1:	C9E6FC777EB4D58A95015DB2514D4BFAC89313DE
SHA-256:	DC21DE8B040CB34995FB62AA46457058596F521098D3B2CAC095A08FCEC92A98

C:\Users\user\AppData\Local\Temp\~DF1C465EC4A4AE6446.TMP	
SHA-512:	5FE904FD43B835659A4B1F07E9BC0877E3A8F27FBD7C4582C1F4D2B9154CEB2C7EDF63DB0DC8D77A1D29326B832BE5C605049250ABDA5CC62661CC9281C753 8
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC3C25805150DF731.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39777
Entropy (8bit):	0.5995582754387802
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR++4y7o2QMcm85DYQMcm85DwQMcm85DB:kBqoxKAuqR++4y7o22NY2Nw2NB
MD5:	B2095C2C316721060BE01F421B27C9DD
SHA1:	9465DF8F9B01A5E81B64595BB1AD251F15BAFB1F
SHA-256:	E047BEE7B9EBBEBFCFA2A048AB19A4DD7B3D7E992E933C4819976B3F29A344EC
SHA-512:	EE366AB60267ECADFDEEDB502249F9E9C4F1865C59D135811DAE83CFDF86C843256745BE9C8389E05CA34EE0FC345906B325070705AF4F789A932DB1EEAF67 1
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 Windows
Entropy (8bit):	6.657199882496558
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:	60e40fb428612.dll
File size:	381440
MD5:	c6bfea479b46b9eb7a69667e0165179f
SHA1:	c7f449ab51a47791a8f3041f0a0dce7c6feb06c4
SHA256:	62dbfe723197430a3af1ec9262fcd2a5c2bfc8e81b97c313101f0a5388d587fc
SHA512:	0ab64d469f20237833da030fce03b44be339e63fc2c3b4a667d1aaa22cf8f6b64cfcf9a2e9314b06fe538ca63ba89465141324ddd603d53971395bc35d6b8ab6
SSDEEP:	6144:vC8nRa6tXFOspzA7n6NZVeC8i795fubASK9beZTX3l8Eo:J0SVOsphVWi7PWoBeZTX36
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~@.....D..... Rich.....PE..L.....S...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x102cd58

General

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	6.63194807603	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
07/06/21-10:14:32.857922	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49732	80	192.168.2.3	40.97.116.82
07/06/21-10:14:32.857922	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49732	80	192.168.2.3	40.97.116.82

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/06/21-10:15:16.513525	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49755	80	192.168.2.3	37.120.222.6
07/06/21-10:15:16.513525	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49755	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 6, 2021 10:14:32.613379955 CEST	192.168.2.3	8.8.8.8	0xf54d	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.669946909 CEST	192.168.2.3	8.8.8.8	0x8172	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.904778957 CEST	192.168.2.3	8.8.8.8	0x8288	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:16.411437035 CEST	192.168.2.3	8.8.8.8	0x3f0f	Standard query (0)	vuredosite.club	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:16.598243952 CEST	192.168.2.3	8.8.8.8	0x198e	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.103801012 CEST	192.168.2.3	8.8.8.8	0xa924	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.104545116 CEST	192.168.2.3	8.8.8.8	0x48	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.106673956 CEST	192.168.2.3	8.8.8.8	0x26e6	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.121890068 CEST	192.168.2.3	8.8.8.8	0x83b1	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.149089098 CEST	192.168.2.3	8.8.8.8	0x3e3b	Standard query (0)	ht.redtube.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.196300983 CEST	192.168.2.3	8.8.8.8	0x3388	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.936816931 CEST	192.168.2.3	8.8.8.8	0x4d70	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:18.986695051 CEST	192.168.2.3	8.8.8.8	0xb8ee	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:19.189786911 CEST	192.168.2.3	8.8.8.8	0xead2	Standard query (0)	ci-ph.rdtcdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:20.643217087 CEST	192.168.2.3	8.8.8.8	0x27a1	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:20.762094975 CEST	192.168.2.3	8.8.8.8	0x2150	Standard query (0)	hw-cdn.trafficjunky.net	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:20.847999096 CEST	192.168.2.3	8.8.8.8	0x45e6	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 10:14:32.659415007 CEST	8.8.8.8	192.168.2.3	0xf54d	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:32.659415007 CEST	8.8.8.8	192.168.2.3	0xf54d	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:32.659415007 CEST	8.8.8.8	192.168.2.3	0xf54d	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:32.659415007 CEST	8.8.8.8	192.168.2.3	0xf54d	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:32.659415007 CEST	8.8.8.8	192.168.2.3	0xf54d	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 10:14:32.659415007 CEST	8.8.8.8	192.168.2.3	0xf54d	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:32.659415007 CEST	8.8.8.8	192.168.2.3	0xf54d	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:32.659415007 CEST	8.8.8.8	192.168.2.3	0xf54d	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.726041079 CEST	8.8.8.8	192.168.2.3	0x8172	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:14:33.726041079 CEST	8.8.8.8	192.168.2.3	0x8172	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:14:33.726041079 CEST	8.8.8.8	192.168.2.3	0x8172	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:14:33.726041079 CEST	8.8.8.8	192.168.2.3	0x8172	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:14:33.726041079 CEST	8.8.8.8	192.168.2.3	0x8172	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.18	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.726041079 CEST	8.8.8.8	192.168.2.3	0x8172	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.2	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.726041079 CEST	8.8.8.8	192.168.2.3	0x8172	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.34	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.726041079 CEST	8.8.8.8	192.168.2.3	0x8172	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.34	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.950735092 CEST	8.8.8.8	192.168.2.3	0x8288	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:14:33.950735092 CEST	8.8.8.8	192.168.2.3	0x8288	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:14:33.950735092 CEST	8.8.8.8	192.168.2.3	0x8288	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:14:33.950735092 CEST	8.8.8.8	192.168.2.3	0x8288	No error (0)	FRA-efz.ms-acdc.office.com		40.101.18.18	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.950735092 CEST	8.8.8.8	192.168.2.3	0x8288	No error (0)	FRA-efz.ms-acdc.office.com		40.101.12.50	A (IP address)	IN (0x0001)
Jul 6, 2021 10:14:33.950735092 CEST	8.8.8.8	192.168.2.3	0x8288	No error (0)	FRA-efz.ms-acdc.office.com		40.101.83.18	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:16.470443010 CEST	8.8.8.8	192.168.2.3	0x3f0f	No error (0)	vuredosite.club		37.120.222.6	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:16.646888971 CEST	8.8.8.8	192.168.2.3	0x198e	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:16.646888971 CEST	8.8.8.8	192.168.2.3	0x198e	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.151671886 CEST	8.8.8.8	192.168.2.3	0x48	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:17.151671886 CEST	8.8.8.8	192.168.2.3	0x48	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.153903961 CEST	8.8.8.8	192.168.2.3	0x26e6	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:17.153903961 CEST	8.8.8.8	192.168.2.3	0x26e6	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.198879004 CEST	8.8.8.8	192.168.2.3	0x3e3b	No error (0)	ht.redtube.com	hubtraffic.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:17.198879004 CEST	8.8.8.8	192.168.2.3	0x3e3b	No error (0)	hubtraffic.com		66.254.114.32	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 10:15:17.246303082 CEST	8.8.8.8	192.168.2.3	0x3388	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:17.246303082 CEST	8.8.8.8	192.168.2.3	0x3388	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.394293070 CEST	8.8.8.8	192.168.2.3	0xa924	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:17.394293070 CEST	8.8.8.8	192.168.2.3	0xa924	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.394293070 CEST	8.8.8.8	192.168.2.3	0xa924	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.394293070 CEST	8.8.8.8	192.168.2.3	0xa924	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.410007954 CEST	8.8.8.8	192.168.2.3	0x83b1	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:17.410007954 CEST	8.8.8.8	192.168.2.3	0x83b1	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.410007954 CEST	8.8.8.8	192.168.2.3	0x83b1	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.410007954 CEST	8.8.8.8	192.168.2.3	0x83b1	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:17.983450890 CEST	8.8.8.8	192.168.2.3	0x4d70	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:17.983450890 CEST	8.8.8.8	192.168.2.3	0x4d70	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:19.047332048 CEST	8.8.8.8	192.168.2.3	0xb8ee	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:19.047332048 CEST	8.8.8.8	192.168.2.3	0xb8ee	No error (0)	stats.l.doubleclick.net		142.250.102.155	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:19.047332048 CEST	8.8.8.8	192.168.2.3	0xb8ee	No error (0)	stats.l.doubleclick.net		142.250.102.157	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:19.047332048 CEST	8.8.8.8	192.168.2.3	0xb8ee	No error (0)	stats.l.doubleclick.net		142.250.102.156	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:19.047332048 CEST	8.8.8.8	192.168.2.3	0xb8ee	No error (0)	stats.l.doubleclick.net		142.250.102.154	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:19.246262074 CEST	8.8.8.8	192.168.2.3	0xead2	No error (0)	ci-ph.rdtcdn.com	cs733.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:19.246262074 CEST	8.8.8.8	192.168.2.3	0xead2	No error (0)	cs733.wpc.rncdn4.com		192.229.221.206	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:20.720418930 CEST	8.8.8.8	192.168.2.3	0x27a1	No error (0)	www.google.de		142.250.201.195	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:20.812123060 CEST	8.8.8.8	192.168.2.3	0x2150	No error (0)	hw-cdn.trafficjunky.net	vip0x055.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 10:15:20.812123060 CEST	8.8.8.8	192.168.2.3	0x2150	No error (0)	vip0x055.ssl.rncdn5.com		205.185.208.85	A (IP address)	IN (0x0001)
Jul 6, 2021 10:15:20.894500017 CEST	8.8.8.8	192.168.2.3	0x45e6	No error (0)	ads.trafficjunky.net		66.254.114.38	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	192.168.2.3	49732	40.97.116.82	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 10:14:32.857922077 CEST	1314	OUT	GET /grower/v6VaX2L98iQ9vNPqP6I1/s7YQ5JAQQXN9djD_2BP/oxHIXx6SfkQXQHWk5gYign/kG_2FSXB9uJKM/uw7wyHm_/2Bzvrq8q92GB9q04QVkch60/s8xolTUIEl/JiLJJpnHLtn3GR9k1/2H8tNCG7sbZq/z7aUK7NADvh/BA6FMpxvpSV9V3/bnPW_2FsZW9JkMS_2Bt_2/FS0OhP_2Bi7_2Fs_/2BndfgWaKsB4v7f/IedJmZ8N1/uc.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 6, 2021 10:14:33.038372993 CEST	1316	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/grower/v6VaX2L98iQ9vNPqP6I1/s7YQ5JAQQXN9djD_2BP/oxHIXx6SfkQXQHWk5gYign/kG_2FSXB9uJKM/uw7wyHm_/2Bzvrq8q92GB9q04QVkch60/s8xolTUIEl/JiLJJpnHLtn3GR9k1/2H8tNCG7sbZq/z7aUK7NADvh/BA6FMpxvpSV9V3/bnPW_2FsZW9JkMS_2Bt_2/FS0OhP_2Bi7_2Fs_/2BndfgWaKsB4v7f/IedJmZ8N1/uc.grow Server: Microsoft-IIS/10.0 request-id: 0c528c66-95f2-66ac-f096-bcb2bbf72a2e X-FEServer: MWHPR13CA0016 X-RequestId: 656c1daf-a33e-463d-94f3-340accd6ebc2 X-Powered-By: ASP.NET X-FEServer: MWHPR13CA0016 Date: Tue, 06 Jul 2021 08:14:32 GMT Connection: close Content-Length: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6680 Parent PID: 5652

General

Start time:	10:13:09
Start date:	06/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\60e40fb428612.dll'
Imagebase:	0x80000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6708 Parent PID: 6680

General

Start time:	10:13:09
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\60e40fb428612.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: 6748 Parent PID: 6680

General

Start time:	10:13:10
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\60e40fb428612.dll,Clockcondition
Imagebase:	0x1320000
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: 6760 Parent PID: 6708

General

Start time:	10:13:10
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\60e40fb428612.dll',#1
Imagebase:	0x1320000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.375971100.00000000053D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.375934102.00000000053D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.375882980.00000000053D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.375768564.00000000053D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.375954554.00000000053D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.375906864.00000000053D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.375822644.00000000053D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.375857537.00000000053D8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6792 Parent PID: 6680

General

Start time:	10:13:14
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\60e40fb428612.dll,Dogwhen
Imagebase:	0x1320000
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: 6804 Parent PID: 6680

General

Start time:	10:13:18
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\60e40fb428612.dll,Sing
Imagebase:	0x1320000
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: 6816 Parent PID: 6680

General

Start time:	10:13:25
Start date:	06/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\60e40fb428612.dll,Wholegray
Imagebase:	0x1320000
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: 6312 Parent PID: 792

General

Start time:	10:14:29
Start date:	06/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6ba990000
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: 1320 Parent PID: 6312

General

Start time:	10:14:30
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6312 CREDAT:17410 /prefetch:2
Imagebase:	0x9e0000
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: 3176 Parent PID: 792

General

Start time:	10:15:14
Start date:	06/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis