ID: 446420
Sample Name: c36.dll
Cookbook: default.jbs
Time: 15:22:18
Date: 09/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

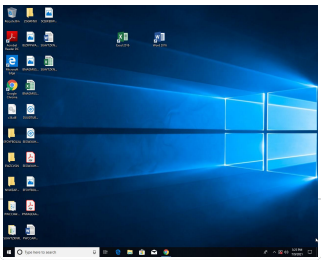
Windows Analysis Report c36.dll

Overview

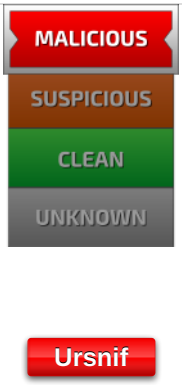
General Information

Sample Name:	c36.dll
Analysis ID:	446420
MD5:	c36ab737db2b6d..
SHA1:	e6fab2798dd6088.
SHA256:	181fe6714ebaff8...
Tags:	dll gozi
Infos:	

Most interesting Screenshot:



Detection

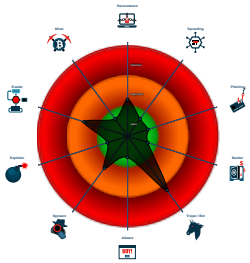


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- 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 dynamically...
- Contains functionality to query CPU ...
- Contains functionality to query locale...
- Contains functionality to read the PEB
- Creates a process in suspended mo...

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4796 cmdline: loaddll32.exe 'C:\Users\user\Desktop\c36.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 1636 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c36.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1844 cmdline: rundll32.exe 'C:\Users\user\Desktop\c36.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1488 cmdline: rundll32.exe C:\Users\user\Desktop\c36.dll,Beautyresult MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1632 cmdline: rundll32.exe C:\Users\user\Desktop\c36.dll,Division MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1948 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1632 -s 852 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5520 cmdline: rundll32.exe C:\Users\user\Desktop\c36.dll,Fastcolor MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2616 cmdline: rundll32.exe C:\Users\user\Desktop\c36.dll,Yetclose MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5468 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3008 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5468 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"1mPXe+HluarwW4R5yJj7kX696atmf6B7a6Jg5mZJ5i3sbRT19R7vT9mKoTtyIRImiHldxTU8DG3omytA0iEqz9hnZgVFnIpVKjKYSqpF7qVSkNASqDhbMdx0CqPxwgtnM3yHiXHYSYrxlGineE5/W0Lx89hsKcfonC8W/kvncnBH4KqU
VMOPQeg/25xF11Xm",
  "c2_domain": [
    "outlook.com",
    "mail.com",
    "taybhctdyehfhgthp2.xyz",
    "thyihjtkylhmhnypp2.xyz"
  ],
  "botnet": "5456",
  "server": "12",
  "serpent_key": "10291029JSRABBIT",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.480154797.00000000039C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.437029493.0000000005A38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.437142340.0000000005A38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.436946677.0000000005A38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.391097194.00000000039C8000.00000004.00000040.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

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

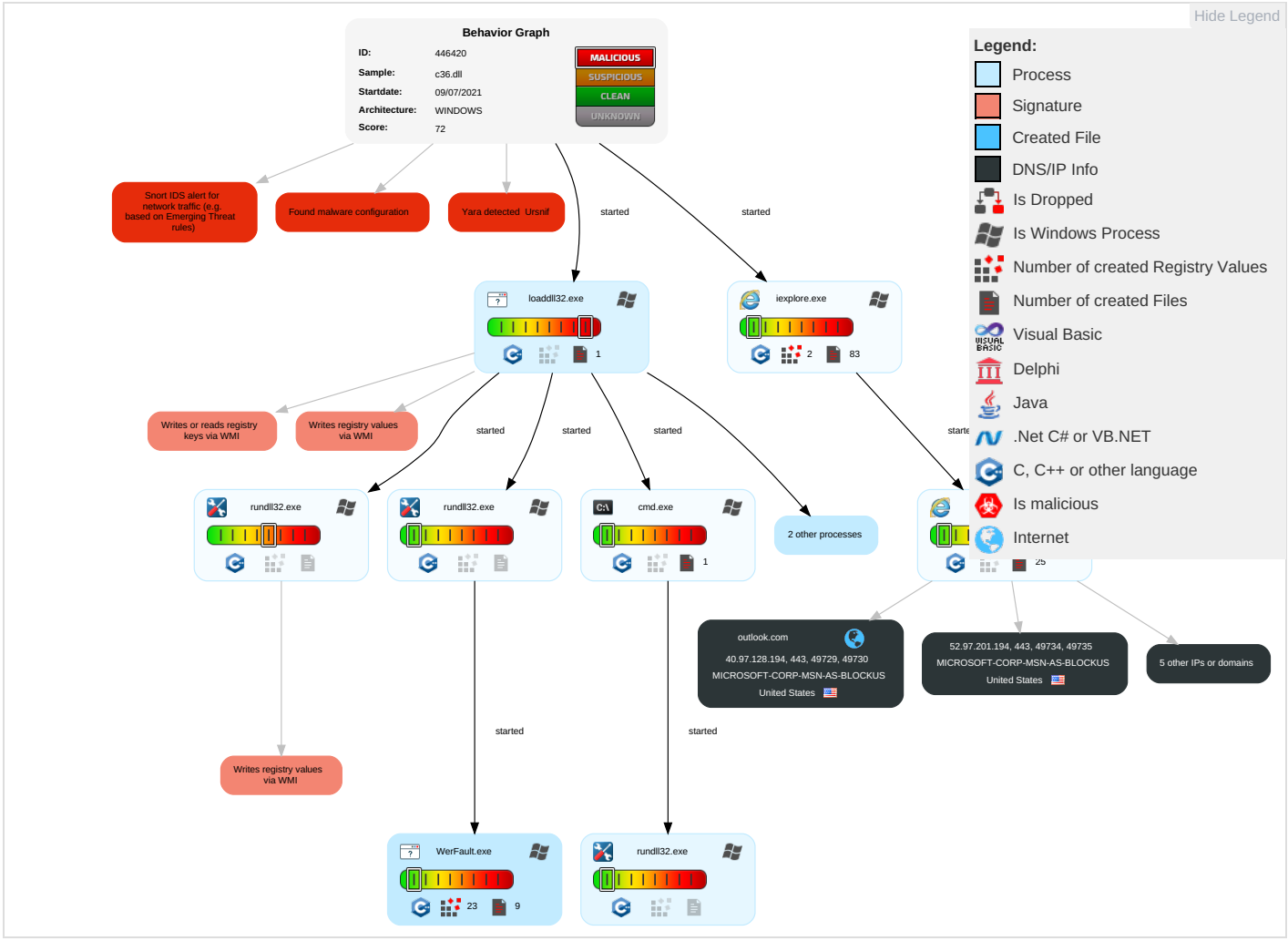
Remote Access Functionality:

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	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 1 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	Remote System 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	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 2 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station

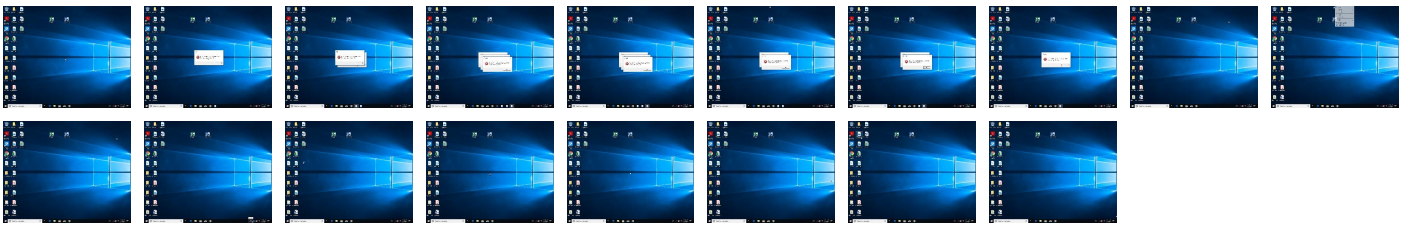
Behavior Graph



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
c36.dll	3%	Metadefender		Browse
c36.dll	14%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.1180000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
2.2.loaddll32.exe.2ea0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

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	52.98.163.18	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/jdraw/D_2BiqNvBbnsXvuMxmM/t9_2FNHkYnKYRDnfwXuIAV/PZdbgLkzH6hzl/QBVRJ_2F/gFwgPVc3A_2BGFDYWcxhxu6/95nq35D0eQ/F_2Bmi0291iuqGJ2R/Lk7llVNKTp1W/ZOLoPeu_2F4/nTZWoYdvVj3RXx/XwwFNQtzd_2FkWk0UpQTO/wz8fmYfCTc8Ok1p_/2Bs3Gpetltr/L74Ig5cboZ/m.crw	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
52.97.201.194	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.98.163.18	ZRH-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:	446420
Start date:	09.07.2021
Start time:	15:22:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c36.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:	34
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:	mal72.troj.winDLL@17/18@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.1% (good quality ratio 14.3%) • Quality average: 79.2% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 80% • 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
15:24:11	API Interceptor	1x Sleep call for process: loaddll32.exe modified
15:24:51	API Interceptor	1x Sleep call for process: WerFault.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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
outlook.com	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
	A1qhcbngFV.exe	Get hash	malicious	Browse	• 104.47.54.36
ZRH-efz.ms-acdc.office.com	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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_kfZ8cLppmcXDuIHKWdMrLPt30SkBa8ipQz83IjjYGp9c2flQixqYXWN470AqCFO8g1yhSwMHhN8-2BJK0vTLNC61PkTeWIrAs821yYsBfCbuclR33OfNLncv-2FtXraICcEYo4WPVv8iupWN7r8K4Ld3UpsglQggrT98vACCXZNhqlBcQYKLRD-2BBljUb02MnMpFHKiH9-2BP5uH3bAOFC4VOgSpVi86N1p2cxRMZF5Xkh4ZdU-3D	Get hash	malicious	Browse	• 52.97.186.114
	http://https://share-ointonlinekcjl5cj5k.et.r.appspot.com/#I.Artolli@sbm.mc	Get hash	malicious	Browse	• 52.97.186.18
	Fund Transfer PDF.htm	Get hash	malicious	Browse	• 52.97.232.194
	http://outlook.com/owa/airmasteraustralia.onmicrosoft.com	Get hash	malicious	Browse	• 52.97.232.226
	http://portal.payrolltooling.net/?id=vpqyydl7ZnKtU4usMGPqUQPtxkGlU49Be%2BH%2BAigE5ucTWat3Eej8US2xdckdOu0iDpwQIwMYKl9DLP2pKOlwIWa7isWu4stPeMJ%2BbSSC%2BrsVtg8U%2BWD1tF4Bc3%2FtEr3hJl4S3OomSDlwnU2PwUDgbmdkRVrT8Jiy8Xe4bfQ0dyp5k2o%2Bf2eztEQzNsZlKz0xjWSRZcdjYCg9vWmNNNSvSwsWNybr8UBeONKYmj4PdCOwhNBWdvur%2BK4Wx1bqcPE26q7z8kpyQ4hJ2vOCvXmdlnZ37w0%2BAGvM3H2V03OaxIsBHrlCuyiPhQWq8qdKOB4lg1EmFibK759dnK%2FawF2z6INf5lJhbtrbLVkWA6i%2FuckBPOJvVXHWYj5SHhB8X%2FZz	Get hash	malicious	Browse	• 52.97.232.194
	okayfreedomwr.exe	Get hash	malicious	Browse	• 52.97.232.194
	Cleared_Payment_Notification_1588-5755.HTml	Get hash	malicious	Browse	• 52.97.232.210
	ORIGINAL.EXE	Get hash	malicious	Browse	• 52.97.186.114

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	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
	Cmh_Fax-Message-3865.html	Get hash	malicious	Browse	• 20.199.16.46
	5.dll	Get hash	malicious	Browse	• 40.97.116.82
	sud-life-mobcast.apk	Get hash	malicious	Browse	• 104.45.180.93
	sud-life-outwork.apk	Get hash	malicious	Browse	• 104.45.180.93
	Flwphoptcdyxlxhpejlfjgmsyzqkhoqweu.exe	Get hash	malicious	Browse	• 20.80.30.45
	2790000.dll	Get hash	malicious	Browse	• 40.101.136.2
	2770174.dll	Get hash	malicious	Browse	• 40.101.136.2
	60e40fb428612.dll	Get hash	malicious	Browse	• 52.97.201.18
	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
MICROSOFT-CORP-MSN-AS-BLOCKUS	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
	Cmh_Fax-Message-3865.html	Get hash	malicious	Browse	• 20.199.16.46
	5.dll	Get hash	malicious	Browse	• 40.97.116.82
	sud-life-mobcast.apk	Get hash	malicious	Browse	• 104.45.180.93

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sud-life-outwork.apk	Get hash	malicious	Browse	• 104.45.180.93
	Flwphoptcdyxlxhpejlfjgmsyzqkhoqweu.exe	Get hash	malicious	Browse	• 20.80.30.45
	2790000.dll	Get hash	malicious	Browse	• 40.101.136.2
	2770174.dll	Get hash	malicious	Browse	• 40.101.136.2
	60e40fb428612.dll	Get hash	malicious	Browse	• 52.97.201.18
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4323c1d7a32576d87639b5d887c5a93fe7aab20_82810a17_06e156cd\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12274
Entropy (8bit):	3.7606060797507106
Encrypted:	false
SSDEEP:	192:orivB0oXSHygO+jed+k/u7skS274ItWcb:sinXqygO+jeR/u7skX4ItWcb
MD5:	E1949ED2D76CA2F7E656F75525C7214A
SHA1:	5B0DE9CE68B04F1D3B9D47663E295C08915D5B48
SHA-256:	E8046A932885BEEB5825A245B4FE4E4D8DF59F8BA5AFF5CE4936E80039FE0BC4
SHA-512:	AC9E9CE727C490D0AC9D14D4EB520D2DB606E8C0FF500801B52F0082CFF2D65E20A9593223CC73249072D8FFD5C72EB932A8ACD3B1985C964B586669EB895F A
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.0.3.4.3.0.8.1.4.0.3.0.4.4.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.0.3.4.3.0.8.8.7.6.2.4.0.4.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.c.c.6.c.e.2.7.-.4.8.f.2.-.4.c.d.a.-.b.b.9.d.-.f.9.7.6.2.5.a.c.d.9.1.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.6.5.e.4.e.5.f.-.1.4.6.7.-.4.0.4.a.-.a.e.2.9.-.f.1.0.6.8.6.6.1.0.8.b.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.6.0.-.0.0.0.1.-.0.0.1.7.-.0.9.5.f.-.1.8.0.2.1.1.7.5.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER301B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Jul 9 22:24:43 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	60620
Entropy (8bit):	1.9423513089497042
Encrypted:	false
SSDEEP:	192:EJWIVZo6IqaxddJaMiFNG9NLtW5CunXlcW8YGUvDcWChpjCOmHtasnomQNqpW:WWI7olJxdbaMZ9FtWs2+WfLc9hCOuRh8
MD5:	1380CF80AF689C5D543F9B1B8986CDD8
SHA1:	B1C78C558C739C72F7196C32387B31CFDBF06761
SHA-256:	817B2C2DE7DBD5A81947B3D95CA0B129979E7A91AD1E91AC40B37C23DBF7ED9D
SHA-512:	F6B2994752EC0B2219832DEE02E10BE6C0A4135D4DE82034F35522ABEC0E8F382F7F26D078B3E2FDC531297A3D1EABEBF685371EBCE554B81D6FC590F922C52
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER301B.tmp.dmp	
Preview:	MDMP..... .....`.....U.....B.....`.....GenuineIntelW.....T.....`...R..`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3ADA.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8298
Entropy (8bit):	3.691360413633455
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLR64pP26Y+V6sygmfTkOSzCpDO89bTOsfkRm:RrlsNi96KP26Yk65gmfTkOSUTNfP
MD5:	FF60444ABF2A813A7A238F2090DDF462
SHA1:	F5F60E50620687E086BA77DE4EC6FBA1244D31E4
SHA-256:	615243FDCD5BE5E6BF8412BB2BCDECE152E85883035283F04323D15B87FB5812
SHA-512:	5A0C913CB7C718C38556DC03EDE5CE97C50EDCFE18703559E07B65ADDCE32761716F13D46BD5A5362C0A0A4EF3BDF438F17741635A9EDA55B749D3ADBC270 29
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.6.3.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DF8.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.450079077396599
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1JgtWI9r6P4WSC8BY8fm8M4JCds9FGx+q8/5q4SrS8ad:uITfPd5SN7JUxhDW/d
MD5:	56585D25B96640D7B66A5F2EBBA9D865
SHA1:	4B804FF08F079C98479A38C534F4851105E50D8C
SHA-256:	DEA4C309F7BE0022283E2B78CFFE988C01CDDCBA96039838674633FD11485029
SHA-512:	ADB806984E748F66AA5AFE42C06BFFD3638B9A3ECD8C364CE6776D7EF08531DDA96D32A3C6524FCEC083A9F84B61417899F834166CDD267C1EC994A2F34188
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1070375" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6C6C1DA9-E104-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7675208968892673
Encrypted:	false
SSDEEP:	48:Iw30GcprZfGwpLjGhG/ap8OtGIpcUwGWGvnZpvUtGogqp9UEGo4hpmUCGWuOEGW+:r3oZZpZjk2OfWUwetUTfU/hMUNoJVB
MD5:	21006F3BE1A506E4B2D3A7D675C3EBDD
SHA1:	4B46C9F4156FBE672987AC7BA44D9E3B12D452AF
SHA-256:	2A15B6133068778BA036876E43A2519E38433920A31EFB23BAA08013BEA921D2
SHA-512:	643BE0C532B07CDF93D7791294D387ED353A34ED50A554C1840E32F350684DBB5A5D7C9DCEF9FD0F3D2A1CE95284A0B6A73EE87B2933E3E991778B0BDFADA3 8
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6C6C1DAB-E104-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27388
Entropy (8bit):	1.8492333825151834
Encrypted:	false
SSDEEP:	96:rpZeQ668BSOj12tWdMBOqQF/9PRqQF/9MpA:rpZeQ668kOj12tWdMBOqCFPRqCF0A
MD5:	FE9CCD814B0F8DDE2AB3DABF6420BE47
SHA1:	4A13D13C7681D3625C0A877A59D47CB2F4F3237D
SHA-256:	C6622CFBD0FC7E8D998683132E490EFC4B9DEDC4AEA47F90409C93C95E014B65
SHA-512:	286A8FE0ABB4D960C91A2628A664236A54FBD90FF60597FE68137E07471D2F212C59DB298B680C2CB752B5F57B2C689120B2C89E422001CB4754183316DAFD53
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):	5.1203165948199825
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE8AeZ7AeZAnWimI002EtM3MHdNMNxOE8AeZ7AeZAnWimI00ObVbkEty:2d6NxOplqSZHKd6NxOplqSZ76b
MD5:	8D599BEF9D241754D23ECCECFD30C7A6
SHA1:	51A406A8931432436C370EA1078E7BE3FA17889D
SHA-256:	2C23AA2A761171E479E8DA74AF011AEDA89AD4ABEE4FAEBF3DD0496EFA5AFE2D
SHA-512:	5B0A837124CE8EDFB3188256F3EE28A78577070A0176CFDE0FB5576D2922AB1340C392BBF7F07683F9108561B46D08579D806E067D7669723E8DC363676DBA38
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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):	5.134563004044832
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k86Z76ZAnWimI002EtM3MHdNMNxe2k86Z76ZAnWimI00Obkak6EtMb:2d6NxrJIfSZHKd6NxrJIfSZ7Aa7b
MD5:	4968B66BBB4A88C515D2C48C5F7D86FE
SHA1:	9A7A7C9FCC6E181E0AC824DB06D7CE4504F7421C
SHA-256:	FE0A0417B43404C5378D17300F8DA55E8A75E852BBE027A5DC3F6D82C0E6ED64
SHA-512:	3EB1E1738241EA8A8D59906A5FBF17E7AA0588C065377687CA8D3FCB791418235D9FC44F3BD016D441AF009FA7FC2C58DC454111186F470A0368D323F88D0362
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x441e92db,0x01d77511</date><accdate>0x441e92db,0x01d77511</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>0x441e92db,0x01d77511</date><accdate>0x441e92db,0x01d77511</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.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):	5.139226419193965
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL8AeZ7AeZAnWimI002EtM3MHdNMNxvL8AeZ7AeZAnWimI00ObmZEtMb:2d6NxvglqSZHKd6NxvglqSZ7mb
MD5:	E65305058781D1E10E76451B366CC50B
SHA1:	A4D4324D1D8A0807B3252A6CC897B2ADAB930F7E

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SHA-256:	248168AC56792FD9991B18F14E4B5AE6117F9BE7AA56800E97BBD5CF7FCFA199
SHA-512:	D9B19329BE9172E086822E4FCA3B21F431C1BC201C992E75FC2DD73D61582628D0A3A38747DE74031E720A52B080F0D691CBEA6F474B76A77427556720CFD091
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.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):	5.136436978120072
Encrypted:	false
SSDEEP:	12:TMHdNMNxi8AeZ7AeZAnWimI002EtM3MHdNMNxi8AeZ7AeZAnWimI00Obd5EtMb:2d6Nx3lqSZHKd6Nx3lqSZ7Jjb
MD5:	C6E669BDEEEAB022234DE6E073CDF6EB
SHA1:	B511F8C524D80A8C2FDFE95BDA8F8D3E0D291F37
SHA-256:	F2CFC7DA7D96C261CEE7A5D4F2A9662543CA5293B05EDDDB9277CDCB077471CC
SHA-512:	7C108964C022559DB1014A2AADACEA1395FBA223B106F846EAFA16B1F1C0675F6B3C6A81B0B51A9DEEC416F8472E6E4AB835B1593953AA771CD4E565CCFAE818
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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):	5.151417094368856
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw8AeZ7AeZAnWimI002EtM3MHdNMNxhGw8AeZ7AeZAnWimI00Ob8K0z:2d6NxQVlqSZHKd6NxQVlqSZ7YKajb
MD5:	BD0CE2FC38BCF545CAB4BE1835DC5E18
SHA1:	A664B1DB83548D55CA28B2EBB79451A2749107D8
SHA-256:	E1C0BED752BBC87034EA8863531BAB3922A3E6F8E08BF981200C17DDEAC8F2A1
SHA-512:	32BB1B156E95FAED8525354D0A145EE4BCFBA0E5DD6FAD8C7EEB6D1BC2BCA147B014C487105261FEB988526A0EE9A16F63F5AF2F7A972C0C8CF78A964F8CB2E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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):	5.123606740322444
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n8AeZ7AeZAnWimI002EtM3MHdNMNx0n8AeZ7AeZAnWimI00ObxEtMb:2d6Nx08lqSZHKd6Nx08lqSZ7nb
MD5:	F3FAA80C08BA5526AB523C40946E247E
SHA1:	6A1E77975DB7D3AC5B0FBE42A3914BD443628F5C
SHA-256:	D449DCB79EC7D2030DFB93AF8BED6A3085BB42166B673476092D78309301A397
SHA-512:	70C9AFB28FDDED7E6F06C56A292AA936CA682F9817102E15EAA8CDEFD8BF472BF822EF8FD47FC1D484CB076D532220B18F39E91E8A0AC3064F0DDC60A9C3CB7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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):	5.160740296090679
Encrypted:	false
SSDEEP:	12:TMHdNMNxx8AeZ7AeZAnWimI002EtM3MHdNMNxx8AeZ7AeZAnWimI00Ob6Kq5EtMb:2d6Nx2lqSZHKd6Nx2lqSZ7ob
MD5:	48714DF7C36784927086738C16F5C2A4
SHA1:	C324557392A9AF2D1AD017801F5FC5A957CC6F52
SHA-256:	C9E7147C35DE4F86CA8D51D49FB2F0814D1782BDD79247FDC593CD315C0DC771
SHA-512:	381DDB57101A933CFDC76B412D6DD4B51EE2FEDF06B865CC560A66CE53FB52B751B458A98A47FCBE46CB7FF2403C44B26508B4A5D9C0B8ABAAF00E48D80F4 8D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.137318022838918
Encrypted:	false
SSDEEP:	12:TMHdNMNxc8AeZ7AeZAnWimI002EtM3MHdNMNxc8AeZ7AeZAnWimI00ObVEtMb:2d6NxRlqSZHKd6NxRlqSZ7Db
MD5:	697674F7D0D805F23E186232B6424E05
SHA1:	DCA130BAD20BDAAF493075711E0FE57A9A3B3E66
SHA-256:	530058573C14408B947F9CD92DCE93C2AFC8277D87440BF8DDF364F3EB4C7A8A
SHA-512:	F04C1267D749CE5230A6C2CD42AADE9847650A33020CA2D7DE18F3D5E0FAC65BD796110DE93F958244D8010E8A955367FBA6878077EF46689E90976C1368724F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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):	5.121867956514355
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn8AeZ7AeZAnWimI002EtM3MHdNMNxfn8AeZ7AeZAnWimI00Obe5EtMb:2d6NxElqSZHKd6NxElqSZ7ijb
MD5:	9A27A88CF938E3C4E0CC0269958A1E58
SHA1:	4D9817EE61624324D4C4B12F44DADC56A0A4C22C
SHA-256:	1AF855867CF3E2A780A6A0446CF441CA6C38DFC5618E08F53A95BF3BDA43E5DC
SHA-512:	84FF9935B33C728DCDE14016A22DB8EABA513D26609A6D3BB865B5388DF4C463750A396A39AA996A17CB2F5ED3B60043C2926F5873E919A3E6B532A3004E8EB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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>0x4425ba91,0x01d77511</date><accdate>0x4425ba91,0x01d77511</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

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.45974266689267
Encrypted:	false
SSDEEP:	3:oVXUTXWQXIqAW8JOGXnETXWQXINCn:o9UbWQj9qEbWQx
MD5:	31F3A28E3C9E0448A4DE020E1CFCE108
SHA1:	7973A0BA483BCDC71D6B4019EED8E339FDD3A4A2
SHA-256:	B996A2D4F7C4BFE8D9768D73D98F5ADBF990DFD46F31592BC98456A97861E47B
SHA-512:	7382AF998560B796D3F4C852AAF037943DE1A7CF13B377A73931DA0318CEE03CA295F950BD7181F66402B667D96651D9B7DA61556C902D6768DD0D68259862D6
Malicious:	false
Preview:	[2021/07/09 15:24:32.452] Latest deploy version: ..[2021/07/09 15:24:32.452] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF07D76F7116EA20F8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39673
Entropy (8bit):	0.5785657953581591
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+djBgDtqQF/9DqQF/9LqQF/9Q:kBqoxKAuqR+djBgDtqCFDqCFLqCFQ
MD5:	43C08021A5463B6D50E11C9B0BAA362B
SHA1:	EDB06BDF34E9CB9AA26AE49B9C86E4CAE07C455D
SHA-256:	1E0EBF8E779D2B155A35E19C0E03DF9BD10B71AF760681FD2EF7B7423CF1F67C
SHA-512:	739BA552A407DF3BE4136C6180ADCC94474DEFCAAEAF689439B218C03F8E6FC00ABD733CA5B80160AC036E3B68D7EC62DA83B91B48FE6BE36119BF8A4565D0F0
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFD1208600E5902E85.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4077520377433156
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lofF9lo99lWBKZuZ5:kBqoIGY0C5
MD5:	CF36976683EF379314E18BCFA7B64F2B
SHA1:	63F70513C6EE4995434753552B1C08602CA2145E
SHA-256:	7194824FCFF90202061DE09AE7017A032227DAC4FA8EDD025BF60BD0B18CAB48
SHA-512:	6EE26E39E72414E447954280B7F418CAB1C9FAB75D7F2254EB5753FA3B4703CED4BFD2F254811B0B72F866800D021EC4C7A43C4CFD9A30CDB269ED402B8BF28A
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):	6.699066149824432
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%

General

File name:	c36.dll
File size:	421376
MD5:	c36ab737db2b6d11fb1f443f8117a7fa
SHA1:	e6fab2798dd6088aa3527a01ae1b3f2415cf40cf
SHA256:	181fe6714ebaff8c1855e8e1dbac545ffd160df0ec96ddf920c5155916b7111b
SHA512:	04884ebda245977509b16eddc89a057582f47cc315610ba040750313bdb668d5377fec118f9c6d7934c7369c3b40d09cb084ec22c71979316ed32860538b0fa9
SSDEEP:	6144:XoiHyepaXa+Cv3FyUtySzhyq++rWM+AVF7tct2PytUDlrfu+U39O:YfGFvFu8hPwM+AVLcMKtKtK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../"j.kC..kC..kC..u...sC..u....C..b;..lC..kC...C..u...RC..u...jC..u...jC..u...jC..RichkC.....PE..L.....+L.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1036ead
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x4C2B8293 [Wed Jun 30 17:44:51 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	9ac2df5a14a0377b217ae274fd22ed43

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x49dbd	0x49e00	False	0.661458333333	data	6.64292711487	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4b000	0x16a65	0x16c00	False	0.650519402473	data	6.09504929451	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x62000	0x998c8	0x1800	False	0.343587239583	data	3.99466653624	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xfc000	0xd80	0xe00	False	0.364397321429	data	3.40694082872	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfd000	0x3928	0x3a00	False	0.554485452586	data	5.40101717847	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
07/09/21-15:24:33.634449	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49729	80	192.168.2.3	40.97.128.194
07/09/21-15:24:33.634449	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49729	80	192.168.2.3	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 9, 2021 15:24:33.469208956 CEST	192.168.2.3	8.8.8.8	0x6450	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.285837889 CEST	192.168.2.3	8.8.8.8	0xcc0b	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.386554956 CEST	192.168.2.3	8.8.8.8	0xa524	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 9, 2021 15:24:33.482678890 CEST	8.8.8.8	192.168.2.3	0x6450	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:33.482678890 CEST	8.8.8.8	192.168.2.3	0x6450	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:33.482678890 CEST	8.8.8.8	192.168.2.3	0x6450	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:33.482678890 CEST	8.8.8.8	192.168.2.3	0x6450	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:33.482678890 CEST	8.8.8.8	192.168.2.3	0x6450	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:33.482678890 CEST	8.8.8.8	192.168.2.3	0x6450	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:33.482678890 CEST	8.8.8.8	192.168.2.3	0x6450	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 9, 2021 15:24:33.482678890 CEST	8.8.8.8	192.168.2.3	0x6450	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.300118923 CEST	8.8.8.8	192.168.2.3	0xcc0b	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 15:24:34.300118923 CEST	8.8.8.8	192.168.2.3	0xcc0b	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 15:24:34.300118923 CEST	8.8.8.8	192.168.2.3	0xcc0b	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 15:24:34.300118923 CEST	8.8.8.8	192.168.2.3	0xcc0b	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 15:24:34.300118923 CEST	8.8.8.8	192.168.2.3	0xcc0b	No error (0)	ZRH-efz.ms-acdc.office.com		52.98.163.18	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.300118923 CEST	8.8.8.8	192.168.2.3	0xcc0b	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.194	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.300118923 CEST	8.8.8.8	192.168.2.3	0xcc0b	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.210	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.300118923 CEST	8.8.8.8	192.168.2.3	0xcc0b	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.232.210	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.399265051 CEST	8.8.8.8	192.168.2.3	0xa524	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 15:24:34.399265051 CEST	8.8.8.8	192.168.2.3	0xa524	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 15:24:34.399265051 CEST	8.8.8.8	192.168.2.3	0xa524	No error (0)	outlook.ms-acdc.office.com	ZRH-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Jul 9, 2021 15:24:34.399265051 CEST	8.8.8.8	192.168.2.3	0xa524	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.194	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.399265051 CEST	8.8.8.8	192.168.2.3	0xa524	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.186.146	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.399265051 CEST	8.8.8.8	192.168.2.3	0xa524	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.186.114	A (IP address)	IN (0x0001)
Jul 9, 2021 15:24:34.399265051 CEST	8.8.8.8	192.168.2.3	0xa524	No error (0)	ZRH-efz.ms-acdc.office.com		52.97.201.210	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	49729	40.97.128.194	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 15:24:33.634449005 CEST	1321	OUT	GET /jdraw/D_2BiqNvBbnsXvuMxmM/t9_2FNHkYnKYRDnfwXuIAV/PZdbgLkzH6hzl/QBVRJ_2F/gFwgPVc3A_2BG FDYWcxhxu6/95nq35D0eQ/F_2Bmi0291iuqGJ2R/Lk7llVNKTp1W/ZOLoPeu_2F4/nTZWoYdvVj3RXx/XwwFNQtzd_ 2FkWk0UpQTO/wz8fmYfCTc8Ok1p_/2Bs3Gpetltr/L74lg5cboZ/m.crw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: outlook.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 9, 2021 15:24:33.761584997 CEST	1322	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/jdraw/D_2BiqNvBbnsXvuMxmM/t9_2FNHkYnKYRDnfwXuIAV/PZdbgLkzH6hzl/QBVRJ_2F/gFwgPVc3A_2BGFDYWcxhxu6/95nq35D0eQ/F_2Bmi0291iuqGJ2R/Lk7llVNKTp1W/ZOLoPeu_2F4/nTZWoYdvVj3RXx/XwwFNQtzd_2FkWk0UpQTO/wz8fmYfCTc8Ok1p_/2Bs3Gpetltr/L74Ig5cboZ/m.crw Server: Microsoft-IIS/10.0 request-id: ae6a76ce-6de3-1bc0-a54d-4b3cc446f95e X-FEServer: DM5PR2201CA0020 X-RequestId: 75af693c-32c0-4f49-a3d1-8caa8be9ee47 X-Powered-By: ASP.NET X-FEServer: DM5PR2201CA0020 Date: Fri, 09 Jul 2021 13:24:33 GMT Connection: close Content-Length: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4796 Parent PID: 5532

General

Start time:	15:23:10
Start date:	09/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\c36.dll'
Imagebase:	0x970000
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: 00000002.00000002.480154797.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.391097194.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.391161462.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.390899688.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.391143928.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.390847636.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.390939253.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.390979627.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.391054400.00000000039C8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 1636 Parent PID: 4796

General

Start time:	15:23:10
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c36.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: 1488 Parent PID: 4796

General

Start time:	15:23:10
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c36.dll,Beautyresult
Imagebase:	0x11b0000
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: 1844 Parent PID: 1636

General

Start time:	15:23:10
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\c36.dll',#1
Imagebase:	0x11b0000
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: 00000005.00000003.437029493.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.437142340.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.436946677.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.482068718.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.437405999.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.437098624.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.437339959.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.436834249.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.437249428.0000000005A38000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 1632 Parent PID: 4796

General

Start time:	15:23:15
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c36.dll,Division
Imagebase:	0x11b0000
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: 5520 Parent PID: 4796

General

Start time:	15:23:19
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c36.dll,Fastcolor
Imagebase:	0x11b0000
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: 2616 Parent PID: 4796

General

Start time:	15:23:24
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c36.dll,Yetclose
Imagebase:	0x11b0000
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: 5468 Parent PID: 792

General

Start time:	15:24:28
Start date:	09/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6d8670000
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: 3008 Parent PID: 5468

General

Start time:	15:24:29
Start date:	09/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5468 CREDAT:17410 /prefetch:2
Imagebase:	0x1170000
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: WerFault.exe PID: 1948 Parent PID: 1632

General

Start time:	15:24:38
Start date:	09/07/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1632 -s 852
Imagebase:	0x1110000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis