

ID: 445525
Sample Name:
bDemJQO51z.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:04:14
Date: 07/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report bDemJQO51z.xlsb 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Memory Dumps 4
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Boot Survival: 5
Hooking and other Techniques for Hiding and Protection: 5
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 21
General 21
File Icon 21
Network Behavior 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTPS Packets 22
Code Manipulations 23
Statistics 23
Behavior 23
System Behavior 23
Analysis Process: EXCEL.EXE PID: 6504 Parent PID: 800 23
General 23
File Activities 23
File Created 24
File Written 24
Registry Activities 24
Key Created 24
Key Value Created 24
Analysis Process: regsvr32.exe PID: 6784 Parent PID: 6504 24

Copyright Joe Security LLC 2021

General 24
File Activities 25
Analysis Process: iexplore.exe PID: 6756 Parent PID: 800 25
General 25
File Activities 25
Registry Activities 25
Analysis Process: iexplore.exe PID: 2240 Parent PID: 6756 26
General 26
File Activities 26
Analysis Process: regsvr32.exe PID: 2432 Parent PID: 6504 26
General 26
Disassembly 26
Code Analysis 26

Copyright Joe Security LLC 2021

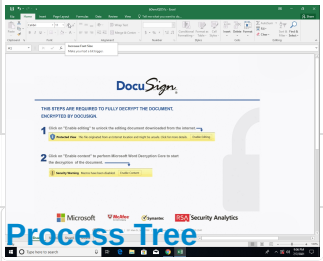
Windows Analysis Report bDemJQO51z.xlsb

Overview

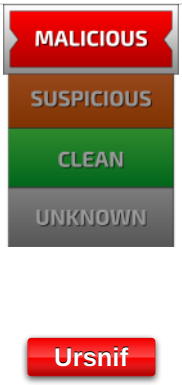
General Information

Sample Name:	bDemJQO51z.xlsb
Analysis ID:	445525
MD5:	b53ed71b3c7a18..
SHA1:	a31f1a98ea227e3.
SHA256:	9e05cd392d9c13..
Tags:	202106221 Gozi ISFB Ursnif xlsb xlsx
Infos:	

Most interesting Screenshot:



Detection

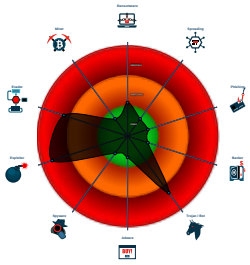


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Multi AV Scanner detection for dropp…
- Office document tries to convince vi…
- System process connects to networ…
- Yara detected Ursnif
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Office process drops PE file
- Performs DNS queries to domains w…
- Sigma detected: Microsoft Office Pr…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6504 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6784 cmdline: regsvr32 -silent ..\tru.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 2432 cmdline: regsvr32 -silent ..\tru.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- iexplore.exe (PID: 6756 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2240 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6756 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.785587738.00000000061C0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.786351947.00000000061C0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.785490720.00000000061C0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.786471515.00000000061C0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000003.00000003.785914746.00000000061C0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 29 entries				

Sigma Overview

System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for dropped file

Software Vulnerabilities:



Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:



Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

System Summary:



Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office process drops PE file

Writes or reads registry keys via WMI

Writes registry values via WMI

Boot Survival:



Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:



Copyright Joe Security LLC 2021

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:



System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information:



Yara detected Ursnif

Remote Access Functionality:

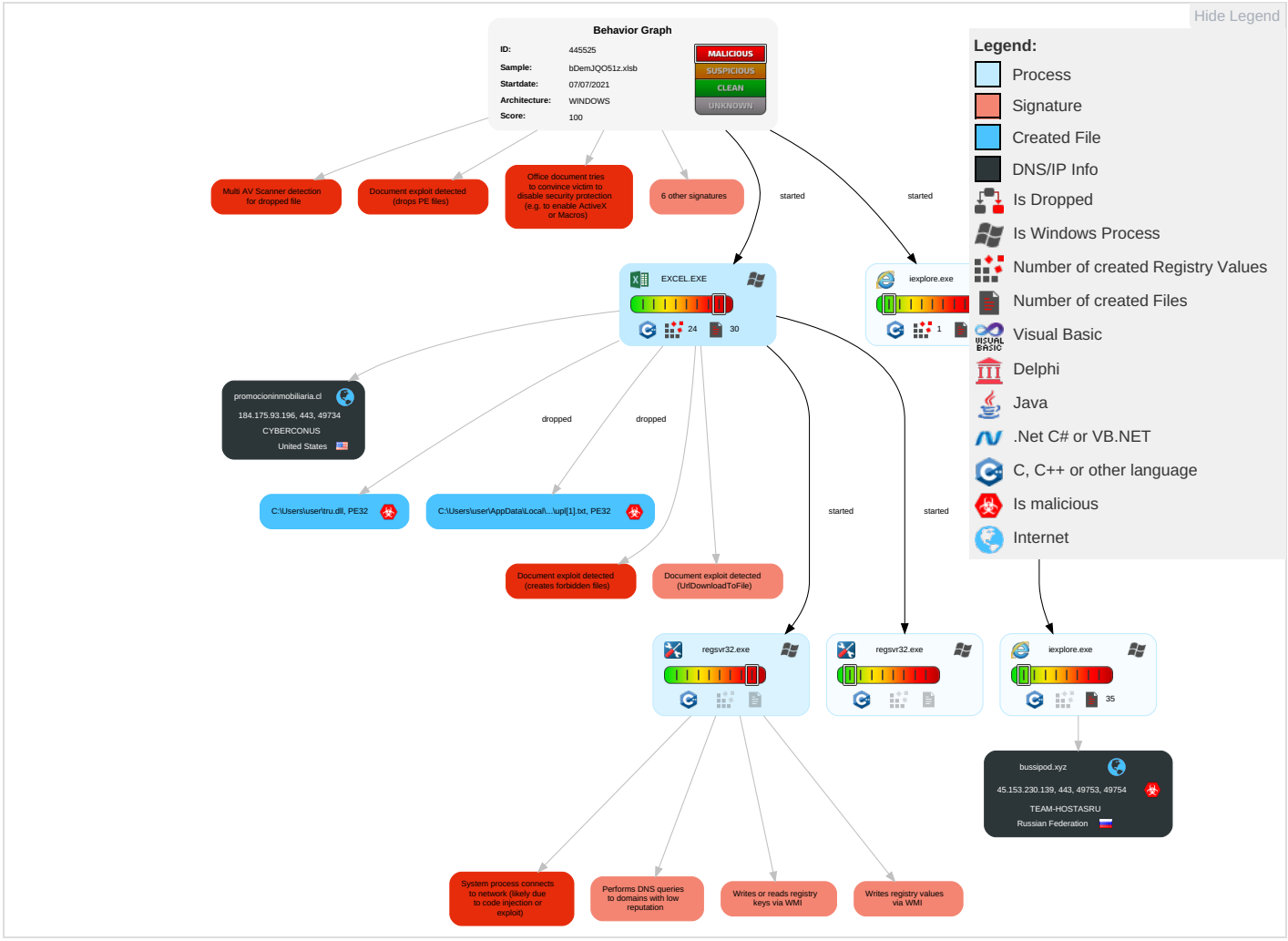


Yara detected Ursnif

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 1 1	DLL Side-Loading 1	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdr Insecure Network Commur
Default Accounts	Exploitation for Client Execution 4	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Regsvr32 1	NTDS	System Information Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

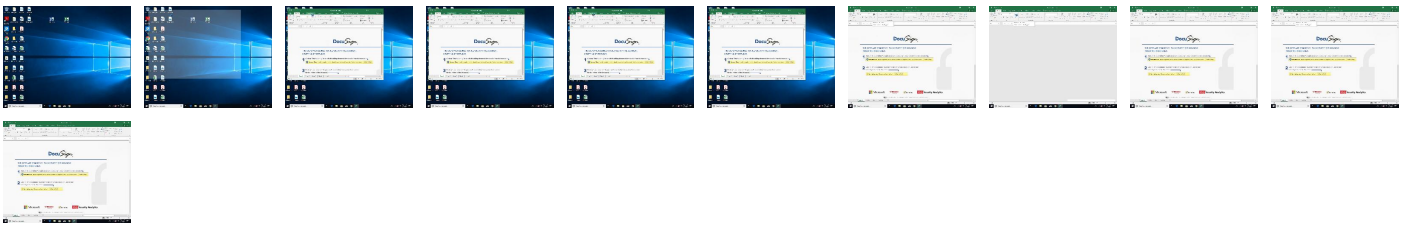
Behavior Graph

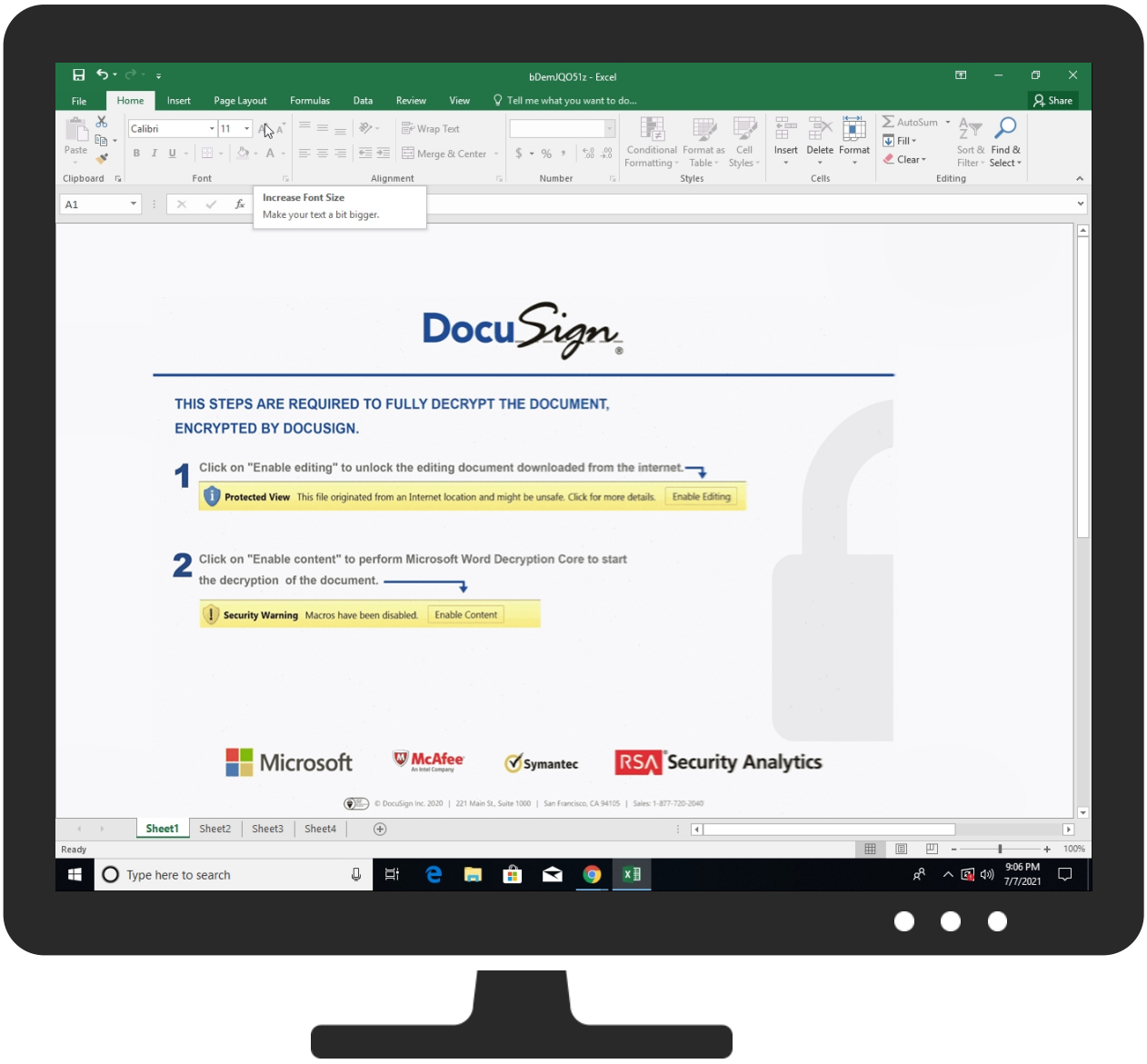


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bDemJQO51z.xlsb	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\upl[1].txt	43%	ReversingLabs	Win32.Trojan.Ursnif	
C:\Users\user\tru.dll	43%	ReversingLabs	Win32.Trojan.Ursnif	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.3.regsvr32.exe.115a1db.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://bussipod.xyz/index.htm	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://bussipod.xyz/index.htmRoot	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://bussipod.xyz/index.htmndex.htm	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://bussipod.xyz	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bussipod.xyz	45.153.230.139	true	true		unknown
promocioninmobiliaria.cl	184.175.93.196	true	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.175.93.196	promocioninmobiliaria.cl	United States		7393	CYBERCONUS	false
45.153.230.139	bussipod.xyz	Russian Federation		202984	TEAM-HOSTASRU	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	445525
Start date:	07.07.2021
Start time:	21:04:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bDemJQO51z.xlsb
Cookbook file name:	defaultwindowsofficecookbook.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:	22
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:	mal100.troj.expl.evad.winXLSB@7/28@3/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:06:28	API Interceptor	2x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CYBERCONUS	5t2CmTUhKc.exe	Get hash	malicious	Browse	• 184.175.83.64
	sample.exe	Get hash	malicious	Browse	• 184.175.106.113
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 184.175.106.113
	ransomware.exe	Get hash	malicious	Browse	• 184.175.106.113
	ransomware.exe	Get hash	malicious	Browse	• 184.175.106.113
	gc79a7rUNV.exe	Get hash	malicious	Browse	• 184.175.106.113
	CONSTANTINE.xlsx	Get hash	malicious	Browse	• 216.15.213.195
	08142020_1463075702.doc	Get hash	malicious	Browse	• 66.201.98.191
	http://srconsultingsrv.com/wp-admin/open-9c-pqmgpgy9fo4mnwz/verifiable-area/10bpikjgd-32105y0ut8/	Get hash	malicious	Browse	• 184.175.123.49
	SecuriteInfo.com.W97m.Downloader.IWY.30727.doc	Get hash	malicious	Browse	• 216.198.213.62
	SecuriteInfo.com.W97m.Downloader.IWY.30727.doc	Get hash	malicious	Browse	• 216.198.213.62
TEAM-HOSTASRU	charge,06.28.2021.doc	Get hash	malicious	Browse	• 45.153.230.72
	legislate.06.21.doc	Get hash	malicious	Browse	• 45.153.230.72
	legislate.06.21.doc	Get hash	malicious	Browse	• 45.153.230.72
	charge,06.28.2021.doc	Get hash	malicious	Browse	• 45.153.230.72
	charge,06.28.2021.doc	Get hash	malicious	Browse	• 45.153.230.72
	decree.06.28.2021.doc	Get hash	malicious	Browse	• 45.153.230.72
	decree.06.28.2021.doc	Get hash	malicious	Browse	• 45.153.230.72
	tell.06.21.doc	Get hash	malicious	Browse	• 45.153.230.72
	tell.06.21.doc	Get hash	malicious	Browse	• 45.153.230.72
	PycwDlq90E.exe	Get hash	malicious	Browse	• 45.139.236.24
	legal paper 06.21.doc	Get hash	malicious	Browse	• 45.153.230.72
	legal paper 06.21.doc	Get hash	malicious	Browse	• 45.153.230.72
	dqVPlpmWYt.exe	Get hash	malicious	Browse	• 185.211.244.128
	4CLq3NmVuR.exe	Get hash	malicious	Browse	• 45.153.230.81
	z5srbx950F.exe	Get hash	malicious	Browse	• 45.153.230.81
	UWiZrKOCXe.exe	Get hash	malicious	Browse	• 45.153.230.81
	4AUzoTtfYq.exe	Get hash	malicious	Browse	• 45.153.230.81
	z4xg3wj6uy.exe	Get hash	malicious	Browse	• 45.153.230.81
	vb2JPIzyc6.exe	Get hash	malicious	Browse	• 45.153.230.81
	ZKMHPZ5Dho.exe	Get hash	malicious	Browse	• 45.153.230.81

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	Cmh_Fax-Message-3865.html	Get hash	malicious	Browse	• 45.153.230.139
	Invoice-Message-7784002.html	Get hash	malicious	Browse	• 45.153.230.139
	Invoice-Message-4821881.html	Get hash	malicious	Browse	• 45.153.230.139
	Mes_Drivers_3.0.4.exe	Get hash	malicious	Browse	• 45.153.230.139
	FAX.HTML	Get hash	malicious	Browse	• 45.153.230.139
	runsys32.dll	Get hash	malicious	Browse	• 45.153.230.139
	Mclawslaw.ca_Fax-Message.html	Get hash	malicious	Browse	• 45.153.230.139
	E00E.dll	Get hash	malicious	Browse	• 45.153.230.139
	Payslip070620219359636Z.html	Get hash	malicious	Browse	• 45.153.230.139
	attach.html	Get hash	malicious	Browse	• 45.153.230.139
	VM52MC9YQDUO0P.html	Get hash	malicious	Browse	• 45.153.230.139
	RFQ40110 (2).html	Get hash	malicious	Browse	• 45.153.230.139
	runsys32.dll	Get hash	malicious	Browse	• 45.153.230.139
	2790000.dll	Get hash	malicious	Browse	• 45.153.230.139
	2770174.dll	Get hash	malicious	Browse	• 45.153.230.139
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 45.153.230.139
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 45.153.230.139
	PO # 2367.html	Get hash	malicious	Browse	• 45.153.230.139
	(1) Voice note-Dassault-aviation.htm	Get hash	malicious	Browse	• 45.153.230.139
	mJSDCeNxFi.exe	Get hash	malicious	Browse	• 45.153.230.139
ce5f3254611a8c095a3d821d44539877	v3EFryEBFV.exe	Get hash	malicious	Browse	• 45.153.230.139
	7favAeMnIv.exe	Get hash	malicious	Browse	• 45.153.230.139
	3MIvJieGXT.exe	Get hash	malicious	Browse	• 45.153.230.139
	SaI1j8jXQY.exe	Get hash	malicious	Browse	• 45.153.230.139
	OMJe815AqT.exe	Get hash	malicious	Browse	• 45.153.230.139
	XGkPj4XMQe.exe	Get hash	malicious	Browse	• 45.153.230.139
	XqsSqSatDk.exe	Get hash	malicious	Browse	• 45.153.230.139
	oxlesp2DxT.exe	Get hash	malicious	Browse	• 45.153.230.139
	Djd7ehHiF8.exe	Get hash	malicious	Browse	• 45.153.230.139
	WHsXHrvbaP.exe	Get hash	malicious	Browse	• 45.153.230.139
	p3Q0iRs6J5.exe	Get hash	malicious	Browse	• 45.153.230.139
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 45.153.230.139
	DhA18Qpbxl.docx	Get hash	malicious	Browse	• 45.153.230.139
	9cYXsscTTT.exe	Get hash	malicious	Browse	• 45.153.230.139
	ibj3mCisBP.exe	Get hash	malicious	Browse	• 45.153.230.139
	ransom.exe	Get hash	malicious	Browse	• 45.153.230.139
	bGk64hnnAZ.exe	Get hash	malicious	Browse	• 45.153.230.139
	aiwXQo9A8t.exe	Get hash	malicious	Browse	• 45.153.230.139
	Main-Setup.exe	Get hash	malicious	Browse	• 45.153.230.139
	mJSDCeNxFi.exe	Get hash	malicious	Browse	• 45.153.230.139

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{643AD4E1-DF56-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7665913312895036
Encrypted:	false
SSDEEP:	48:IwWGcprnGwpLjG/ap8YGIpcfGvnZpvyGoTPqp98Go435zpmEGWT5fTYGWT7T6pOK:rKZxZD24WwtYifn35zMMRs6KFBLSpB
MD5:	F1E8391B91C8FD98A4DCDB797345F37A
SHA1:	3052D424084701BDB5765112C5C77A83A781B31C
SHA-256:	49DF2C9D24D64FCF47492D2A57B695A2F3A4DA2BA9BC3E8C6D24C10A55542195

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{643AD4E1-DF56-11EB-90EB-ECF4BBEA1588}.dat	
SHA-512:	D952B2E173C99C48575BA01B4BC3CB9FDB654FAF7C7DF5402FEF37B3AA8BBE2075F5B8700E332FE60B8F28DB0BF6FB48EC7B06C363E68FFA64803D021910B7D
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\{643AD4E3-DF56-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26248
Entropy (8bit):	1.6580929366922152
Encrypted:	false
SSDEEP:	48:IwuGcprvGwpanG4pQzGrapbSIGQpB2GHHpcLTGUp8VGGzYpmY5FGopaqZ8fGA/X/:ryZZQJ6XBSwj12lWkM4wP/VSA
MD5:	3BEB5DAA27A7AF27EE5DB0C3210FBD20
SHA1:	479196CFFCD9608E276AD3AF8BBAA5A955CAA5BB
SHA-256:	422DDE71533CF70C4DC47E9EE799198525DFA2855D7C7E85B7B9C2E7383F27CB
SHA-512:	8BDF2D62BF9A05FF063AA1B2464DDE8EE23041EA6F7C2A95751216980D289446E40D7514B4A9B66A51435F4D664D4645B6DE4414CE0683DE2ED84816A8C7D6C
Malicious:	false
Reputation:	low
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):	5.059958773870817
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE7nWimI002EtM3MHdNMNxOE7nWimI00OYGVbkEtMb:2d6NxOuSZHKd6NxOuSZ7YLb
MD5:	B41CF8C50222AD4A456F23ABB0B6F6FC
SHA1:	1D462336AC7E5FB1A2EA2077E2016DCF6C0D5294
SHA-256:	082E2C5FF39658A1E04EDAC4A6FB04680507D43C8310824AB7C2B64D4172CB61
SHA-512:	BD55121CEC1995341C34B21814D42184439CE4CC06D660837B05E00670BA517C03D0BA9D8F040FFBEA612C71DB76EE54CEFC628F1F34F80E7685F091AD208AD
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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):	5.094312040833597
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kpnWimI002EtM3MHdNMNxe2kpnWimI00OYGkak6EtMb:2d6Nxr0SZHKd6Nxr0SZ7Yza7b
MD5:	F19D37AE906CA5A41FF7B92ED34AA2D7
SHA1:	23C2D6872336923AC6A8B589A2D0562AAAC70772
SHA-256:	8882C3D8BFD443749D834D8C5594EC83A406574AF25E3E1E974C226F871CAE9A
SHA-512:	68DC388574A5E9B8CF13C504535CBC57CD740BC466960E3FB3C0E362D45488DD8062F7B167CA043C416E7AC8D4A1A69CE030D45CAC1B62DFD9F416C3F55586C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x3abe3f20,0x01d77363</date><accdate>0x3abe3f20,0x01d77363</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>0x3abe3f20,0x01d77363</date><accdate>0x3abe3f20,0x01d77363</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):	5.079699573594208
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL7nWimI002EtM3MHdNMNxvL7nWimI00OYGmZEtMb:2d6NxvnSZHKd6NxvnSZ7Yjb
MD5:	8AE6253D6E6A8F81CB750B0D48347479
SHA1:	AC4EDC386DFEF7EB8D4465D56E2F9DC473A5FDA5
SHA-256:	724C144C8488BD0C76F180C927CC42D33248DB7272DE65DB9F623BFC68417601
SHA-512:	7DBE3D5F5E1CC42E0F5B985FB8B9EF53E27CD89D7C991E931D232294C0AA1A924EC5E57108E7F97C72C3CE1DA24BD4FB6E51E98EE53EFC4C57026B5A0D2D213
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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):	5.07494825240439
Encrypted:	false
SSDEEP:	12:TMHdNMNxi7nWimI002EtM3MHdNMNxi7nWimI00OYGd5EtMb:2d6NxESZHKd6NxESZ7YEjb
MD5:	7C5CC47CBC2F6D5FC74CDC5860642917
SHA1:	D72FE627600977DA7C90379A8D9F6CE63DB1CF61
SHA-256:	0ED9C19F3DDA7781DE64F975E0818199E2D8484CE929D59A2BD41BAD70219FEB
SHA-512:	D640383112D698275CB50C78133B9D5479223CA2CDF2FC4FA786554BAD0909300D34F8652256F5EC587D020FB6D7CA10D8E7B034F4303396879FF68B21B73C02
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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):	5.094260227035077
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw7nWimI002EtM3MHdNMNxhGw7nWimI00OYG8K075EtMb:2d6NxQCSZHKd6NxQCSZ7YrKajb
MD5:	10EF638595F68E547C08F53819032B4D
SHA1:	FDC07D127A5412DB64156446A0E550FCF1FE200A
SHA-256:	08B8700E162CB35797860AF87A589544BA3E699F090FA0DF0CFAFBFB81C2A586
SHA-512:	02B4A327D7DF549F56DE79B74B7832FBC96A6D753EB30939ACE20E815EC2454F0B03E57F3033E6803B17D68602AF0175C6D80FAB1449DF25BF4EA1712E173657
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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):	5.063564934558767
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n7nWimI002EtM3MHdNMNx0n7nWimI00OYGxEtMb:2d6Nx07SZHKd6Nx07SZ7Ygb
MD5:	BE54AB7DEC291AC84BF444479821B35F
SHA1:	6262053617300CD13C67530B6EC02CFB5228EEF5
SHA-256:	FEEFA73FFB62C5BE6B8520B0FC825796202F3EE7F5AFA240F65DFCABBE97834E
SHA-512:	8D860B9FBC9CF4F1EA59EEB189ADD8B69205FE7B18B66F866C8D080CB4B6A404B5FBDB92039D10920DA1FF578F3DF40E46530D79EB7018FDA8F57F80C7F95D1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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):	5.099594053198611
Encrypted:	false
SSDEEP:	12:TMHdNMNxx7nWimI002EtM3MHdNMNxx7nWimI00OYG6Kq5EtMb:2d6NxdSZHKd6NxdSZ7Yhb
MD5:	2CDC4B1296F4F103FCD21A8E8A314EAA
SHA1:	BC56BC07155564D442CC08143408D5CA7B8C472B
SHA-256:	8003328BB194573A9CBF71CDB70448AB16676A92C16262761468FF5C2FA90B3A
SHA-512:	1504FFF674D8F5D02D20905FAAA4A3AD1276AFA31DC91ABD1773CB3376BC895C1EC6525B53EF3B962CBE84B171C6CFCE72CFF6054079621510CCDC6445A3D7F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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):	5.082959143332767
Encrypted:	false
SSDEEP:	12:TMHdNMNxcpnWimI002EtM3MHdNMNxcpnWimI00OYGVEtMb:2d6NxcSZHKd6NxcSZ7Ykb
MD5:	377295D6B628CC755B3AC0177138DA0E
SHA1:	E068B500141A936CB7779F74D54E936FF4AE41A2
SHA-256:	5D24E9B2A1534ECFD0FB1017D4B33DFE3F310268795A650088C3DA96F22D3778
SHA-512:	682BD8347130F94404CFAB6590DCE12AADE402E534FDA2EFC4CBCF0437868E7872A9138C97C3F8C976919FD01F3BC3B664D567114B84316A820B5A9351715065
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x3abe3f20,0x01d77363</date><accdate>0x3abe3f20,0x01d77363</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>0x3abe3f20,0x01d77363</date><accdate>0x3abe3f20,0x01d77363</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):	5.060607950760631
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn7nWimI002EtM3MHdNMNxfn7nWimI00OYGe5EtMb:2d6NxjSZHKd6NxjSZ7YLjb

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
MD5:	3DCF9C0C2B4980F59DCC198D38C6AD17
SHA1:	8F0C59E242BF79BAFD5CA8DAE0BD695BC466D57C
SHA-256:	3CFA1DC26AED6D71B0EF201D6F1E076E271D3D9B862C72D6C1ECFD170EBBA618
SHA-512:	81A206CF07ED3A707792465FC05676B4CFC5AD62527A8170DE20DB0632937E09DF894E2467DFD9FCB25B6A57DB61876FFB526726B4CADFB3B0203FF9CBD8482
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</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>0x3ac5e040,0x01d77363</date><accdate>0x3ac5e040,0x01d77363</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E3EB9BFB-9A3C-4BB8-990C-FB40D6108524	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	135209
Entropy (8bit):	5.36308595211387
Encrypted:	false
SSDEEP:	1536:GcQIKNgeBTA3gBwlpQ9DQW+zoY34ZliKWXboOidX5E6LWME9:gEQ9DQW+zwXO1
MD5:	22390383207807ECE713F2FD66074C26
SHA1:	DC04617F16883BC64D5C2B4673BDE78E6091E5ED
SHA-256:	E3E606F2F9AA0744A0F380431FB62A954F02E6C5824317A72FE25DCFD403A320
SHA-512:	6D19195158D97CC637D54EFB5482287BA0DBD87CB5F861FAF9E5231A8B03A6433A6F8E3D8DAD5CD64ABC0FBFCD91C81DCC3AF58F8AF110D1A010B2D1847C4DF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-07-07T19:05:14">.. Build: 16.0.14306.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\51A62567.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 8 x 10, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	176
Entropy (8bit):	6.077353107923878
Encrypted:	false
SSDEEP:	3:yionv//thPlvtt2Lts2jh/rywOZx9yTl+RESJiWiy8Z1n/XUKTeg1p:6v/lhPgRFjhmhyoiSQZRUAdp
MD5:	E9BFB9B9FCBAC9F66AA5D02237A83073
SHA1:	5F602C8214375078A7E503E070FDD1DBE44B30C3
SHA-256:	23D4BFA6C8893A9C3570C26A1973641A71C787B36B32C6BE64F0DEE8584C86E4
SHA-512:	17A77897B0C5134CEB6AC39D624388553A13CE20974C3FF858DD1044FB743A71D35208B9487B429CCC8CD89126DC49F9F191C6113C63A0E88D7AF43B9AF62F2
Malicious:	false
Preview:	.PNG.....IHDR.....sRGB.....pHYs.....+.....UIDAT.W].A..0.....`....C.....{}.g@..RW=.q^q.=.....<...=.r..l.q.x..\x._V9^..D...E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FF65F03C.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 922 x 684, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	422520
Entropy (8bit):	**7.996314840104008**
Encrypted:	**true**
SSDEEP:	12288:WtZp/w4fvVUUcXGS2qBhQbdOM2lCLtTWAUrbIqjx9E5T:WxoYVUrb2NOQtTWAUvrj3CT
MD5:	24BA12C8BF662394E56B372B046A9EBA
SHA1:	E244001DB714FEA1AB5D87AB4E5820208A15CF62
SHA-256:	1D42F50610C56E2816FFC0BF036C75CDD9E3008F9810DBD25644E3482AACFA42
SHA-512:	C7BEED250A505F5EB8ACCE734525B3D92AA0C95F454C8B2C0D48DE5AD41193CD8174E94B47D9DF0A61A8FC8C8AF549FCBDC493DE73CDDF967E64BE484254AFB
Malicious:	false
Preview:	.PNG.....IHDR.....U.....sRGB.....pHYs.....+.....IDATx^....eGu-:.{r.i.f4.0A9K.PBB`@....6.8`.N..`?g..`.19J$.BX..s.i.&I....9u.....z..U.[..yX...u..^{.Uu.{nSOO.q....jjj.w...@ss3.....n.9.7.9e...R.<k..j.`=.....Q...M}...n<m~.B.s.@%.e[z.....M.>.l.c.....6#.....'._....?.\,..Y....OT.s.b..7...K?[^....$..e.f"..bl"....../kdx.\..E.....1.....G...=y.d3....d...6(L.....x.+c..$.....Z.G...o.c.....)...E..#...%...(...#;..O/.2~.0,....5....._%....K.....t.8.a.....1..%d,.....(..I.....|...z....L...h.....(A4.2.TJf.]..SS%k...d....I.,.....%.....jIDT6.S...6.Id..[_.z..o..1j...."...1C.|.;E....2.G....e9..$...].!Cv.@}.x..o<n...|....Y..>.....[.q....*.T1.xQ.{...u..Y.gI..Aew.C..Q?b..?[nZ.O...h.X.....F.....K.I.....A....R.Pi....`K.x..j8...:..2.\.e.+N!.....q'.....(E(.i.gK#E.n&A..nv..A..5r...?.H.A.....g.....#Pbx,.....J...U4...-....9..9.).....Dd...T.X..F..C..zx.b..."j.D...d.&jE.~.....R.T.%...25.dqe..` ..M.....d.Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	dropped
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Preview:	......JFIF.....d.d......Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\upl[1].txt	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	404992
Entropy (8bit):	6.667040453584233
Encrypted:	false
SSDEEP:	6144:h8vockvtMD67Dvy8CyOuq107KjWMTxdtcrsianUAqPt/MmG3G/GERIgg:SwhtCy50mpMTxdtV8AqPtM3gN
MD5:	5522C21A05DAF91658951BDF1C0E5271
SHA1:	FED4A9B4069CD2676928441ECF8C844CC7F4A9EE
SHA-256:	EB6E2519AA5C31174A1ED6C0193B2D0E49E9ED6CA1AC01ED94B3007B5E2F6993
SHA-512:	D97A8021B9688C612E280FFCB5443916B9D09857DAF82A62BD5EFAC35EFEFF138125466A74579568DD655CD66CD5085E10CEDB4CAF7981F4EE9F240839B33D5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 43%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f..."..."..."......:.#...<.9.7...</.....+.?.+..."...V...<.(.....<.>.#...<.8.#...<.=.#...Rich".....PE..L....6JJ.....!.....d...r.....MQ.....@.....4...d..... .....|".. .....@..... .....text....b.....d..... ..`.rdata...f.....h...h.....@..@.data.....@....rsrc... .....@..@.reloc...5.....6.....@..B. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ErrorPageTemplate[1]	
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKlv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}I$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;.,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.4382905670638335
Encrypted:	false
SSDEEP:	3:oVXUdXUfF7W8JOGXnEdXUfFgn:o9UVUf0qEVUfm
MD5:	22530EC16123D69F6BBD980485593697
SHA1:	5E260BFEC0131704952EDFDEBED95EB6E0002113
SHA-256:	919D40AA995D1A4B1191646E0B503051E20F9C3CF834F382971EF0F9B5FAC5E7
SHA-512:	9BBBD41DE0804B218D1FBD7095E40432EF609EB5EB859E9B479B51DC434558B87D17E752B6C1D1A4641B202E2DCCCEB4F5D9C96ACA54B31FF938D77EFF5FB579
Malicious:	false
Preview:	[2021/07/07 21:06:12.934] Latest deploy version: ..[2021/07/07 21:06:12.934] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF5838B134AEB34B2C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38745
Entropy (8bit):	0.37169551383082305
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+Jn1kYIYkqZ8uqZ8QqZ8d:kBqoxKAuvScS+Jn1kHb2I1
MD5:	1864878A8F36324C7D867F6CB684DE4B
SHA1:	17C4C72FDDE876AC609B0808A6AB07B37CC67E55

C:\Users\user\AppData\Local\Temp\~DF5838B134AEB34B2C.TMP	
SHA-256:	DFE45CB395C85131AD5540CE07004125A1FED955440AC573C2C2E3FD60B5D6EE
SHA-512:	0475600736E8385A432A3B136FFE6B7CD45301D1BED42DF0F2A51BED1EE668344E7028806FEA367BE425FB240620199FF170318B1E1D260F2EEFE38015488FB4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.991532360136052
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	bDemJQO51z.xlsb
File size:	437796
MD5:	b53ed71b3c7a18f70d693a137b5adc5c
SHA1:	a31f1a98ea227e331303ec0c6ee226a711427998
SHA256:	9e05cd392d9c1334c404ceb8fe28d6bc179d9844569bced9d2d1c057de538dee
SHA512:	0c528acb14396cd98cd7ff4516a13744ba90cd07b28a9badc6142bccaa4542e4e23acba888f0eb872eb8252a8c65cd39262bae0ce4f41d7dad637613c9c918ae
SSDEEP:	12288:6EtZp/w4fvVUUcXGS2qBhQbdOM2lCLtTWAUrblqjx9E59:6ExoYVUrb2NOQtTWAUvrj3C9
File Content Preview:	PK.....!.....[Content_Types].xml ...(.....!!..... ....

File Icon



Icon Hash:	74f0d0d2c6d6d0f4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 7, 2021 21:05:16.669984102 CEST	192.168.2.4	8.8.8.8	0x3c70	Standard query (0)	promocioni nmobiliaria.cl	A (IP address)	IN (0x0001)
Jul 7, 2021 21:06:14.290328979 CEST	192.168.2.4	8.8.8.8	0x38dc	Standard query (0)	bussipod.xyz	A (IP address)	IN (0x0001)
Jul 7, 2021 21:06:27.262942076 CEST	192.168.2.4	8.8.8.8	0x4e0b	Standard query (0)	bussipod.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 7, 2021 21:05:16.979497910 CEST	8.8.8.8	192.168.2.4	0x3c70	No error (0)	promocioni nmobiliaria.cl		184.175.93.196	A (IP address)	IN (0x0001)
Jul 7, 2021 21:06:14.349544048 CEST	8.8.8.8	192.168.2.4	0x38dc	No error (0)	bussipod.xyz		45.153.230.139	A (IP address)	IN (0x0001)
Jul 7, 2021 21:06:27.318104982 CEST	8.8.8.8	192.168.2.4	0x4e0b	No error (0)	bussipod.xyz		45.153.230.139	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

HTTPS Packets

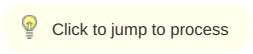
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 7, 2021 21:05:17.367516994 CEST	184.175.93.196	443	192.168.2.4	49734	CN=promocioninmobiliaria.cl CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat May 22 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Aug 21 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 7, 2021 21:06:14.466537952 CEST	45.153.230.139	443	192.168.2.4	49753	CN=bussipod.xyz CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jun 28 14:38:28 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Sep 26 14:38:27 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jul 7, 2021 21:06:14.467595100 CEST	45.153.230.139	443	192.168.2.4	49754	CN=bussipod.xyz CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jun 28 14:38:28 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Sep 26 14:38:27 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 7, 2021 21:06:27.420726061 CEST	45.153.230.139	443	192.168.2.4	49760	CN=bussipod.xyz CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jun 28 14:38:28 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Sep 26 14:38:27 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6504 Parent PID: 800

General

Start time:	21:05:12
Start date:	07/07/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xcc0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Copyright Joe Security LLC 2021

File Created

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 6784 Parent PID: 6504

General

Start time:	21:05:18
Start date:	07/07/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -silent ..\tru.dll
Imagebase:	0x1180000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785587738.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786351947.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785490720.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786471515.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785914746.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786046396.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785681429.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785395370.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786832498.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786290579.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786111301.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786598638.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786404919.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786951850.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786858058.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786925101.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786757271.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security

	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786687841.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786643583.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786530397.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786910689.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786941081.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786803854.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786882909.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786722388.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785763994.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785197460.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.793270555.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786173982.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785302233.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785981820.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.785845872.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.786231862.00000000061C0000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6756 Parent PID: 800

General

Start time:	21:06:11
Start date:	07/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff636db0000
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: 2240 Parent PID: 6756

General

Start time:	21:06:12
Start date:	07/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6756 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: regsvr32.exe PID: 2432 Parent PID: 6504

General

Start time:	21:06:37
Start date:	07/07/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -silent ..\tru.dll
Imagebase:	0x1180000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021