ID: 500413
Sample Name:
616412739e268.dll
Cookbook: default.jbs
Time: 00:35:10
Date: 12/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report 616412739e268.dll

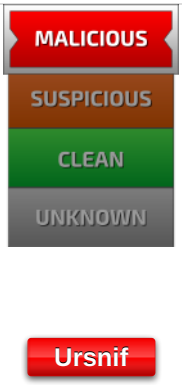
Overview

General Information

Sample Name:	616412739e268.dll
Analysis ID:	500413
MD5:	9e67e68ddbedba..
SHA1:	f2c7b0735343081.
SHA256:	41c0934ba1be03..
Tags:	brt dll gozi isfb ursnif
Infos:	

Most interesting Screenshot:

Detection

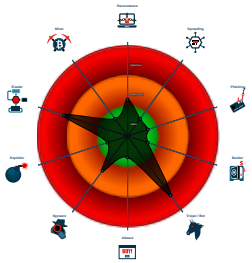


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Multi AV Scanner detection for doma…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Uses 32bit PE files
- One or more processes crash
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7036 cmdline: loaddll32.exe 'C:\Users\user\Desktop\616412739e268.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 7040 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\616412739e268.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7052 cmdline: rundll32.exe 'C:\Users\user\Desktop\616412739e268.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7072 cmdline: rundll32.exe C:\Users\user\Desktop\616412739e268.dll,BeGrass MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6452 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7072 -s 636 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 1364 cmdline: rundll32.exe C:\Users\user\Desktop\616412739e268.dll,Fieldeight MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6824 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1364 -s 644 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6464 cmdline: rundll32.exe C:\Users\user\Desktop\616412739e268.dll,Often MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6368 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6464 -s 632 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"UmEkthy8LQToWYBqtBaWyLn/P1d2KjpXi9nl2is1X7NEi7AW4Al92U7HvBiCwWHgXhs6UyTZ7q6npv3YCi+rPS7xAyorWWgcyyviEpE9CETDXviZ72XZkxmen4ztvEtct+obFAEe0tiXOsfOcC8xDsI0CHPpvmUknsexTYqAJgwcghgx
1mGHx/yFM4fnPYw4mFFE6bVI7eMnbu1CuunRmAVRDHZ7MAS7zSkAmYjeo1zAzRnOEWgblRHwenmwlBtp0SFGuYCGVe3TZZ4NndgpdSxpSeLOoSZi/fRXjtS8b6LXBS/zslRCRObMDjDX4pa1fM1uOgFHyvjANgWJpZ272bpOHjM52/hsE
GZXskaNztU=",
  "c2_domain": [
    "msn.com/mail",
    "breuranel.website",
    "outlook.com/signup",
    "areuranel.website"
  ],
  "botnet": "8899",
  "server": "12",
  "serpent_key": "56473871MNTYAIDA",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.916793229.0000000003BB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.916426520.0000000003BB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.974874720.000000000573B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.916847995.0000000003BB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.855981301.0000000002EC0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.rundll32.exe.8aa31a.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.322a31a.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.3.rundll32.exe.2eca31a.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.3.rundll32.exe.2eca31a.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.342a31a.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Networking:

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

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

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

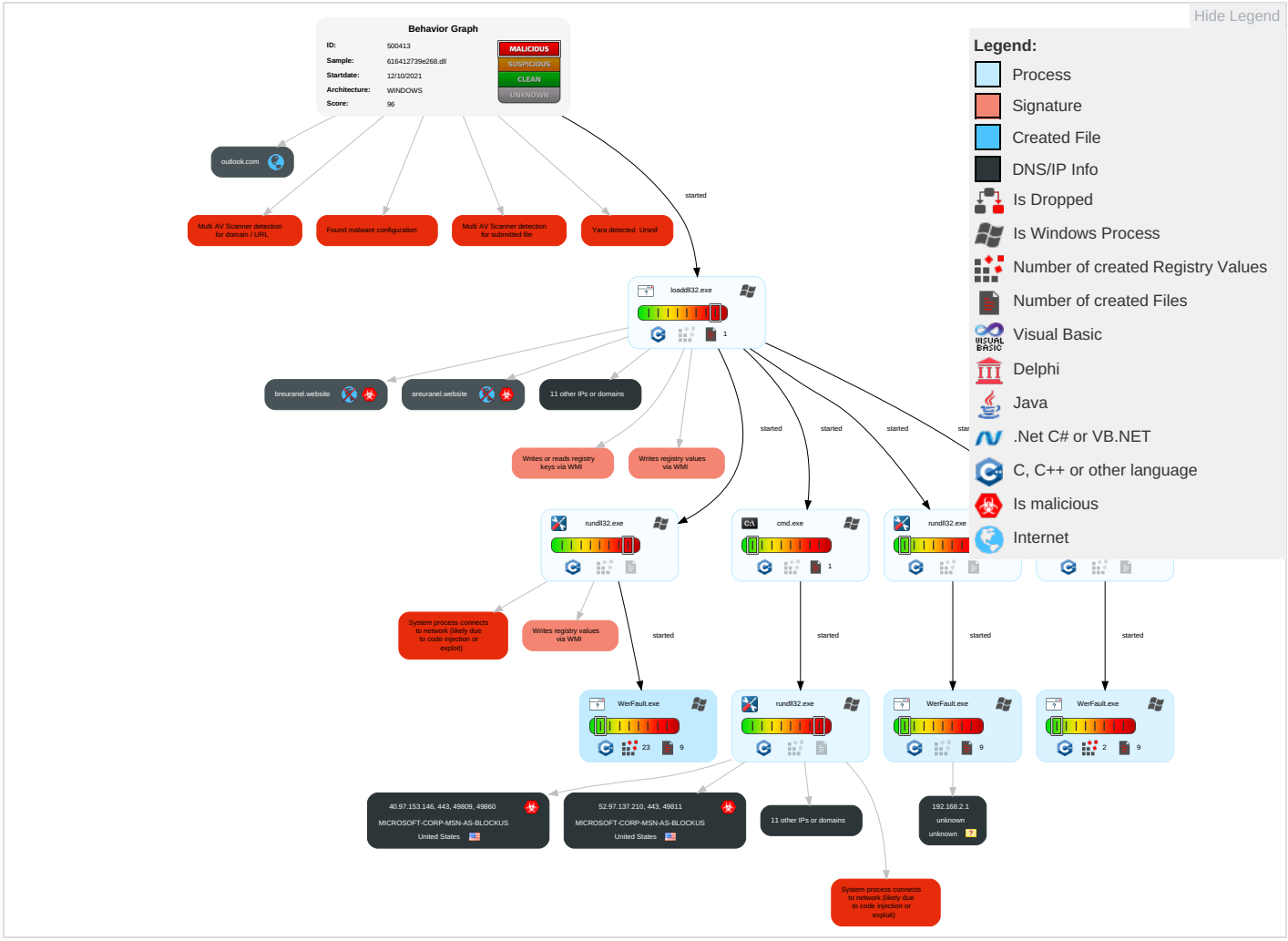
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 1 2	Virtualization/Sandbox Evasion 1	Input Capture 1	System Time Discovery 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eaves Insec Netw Comm
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1 2	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Locat
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 1 4	SIM C 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	Manip Devic Comm
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	Jamm Denia Servic
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	Rogu Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

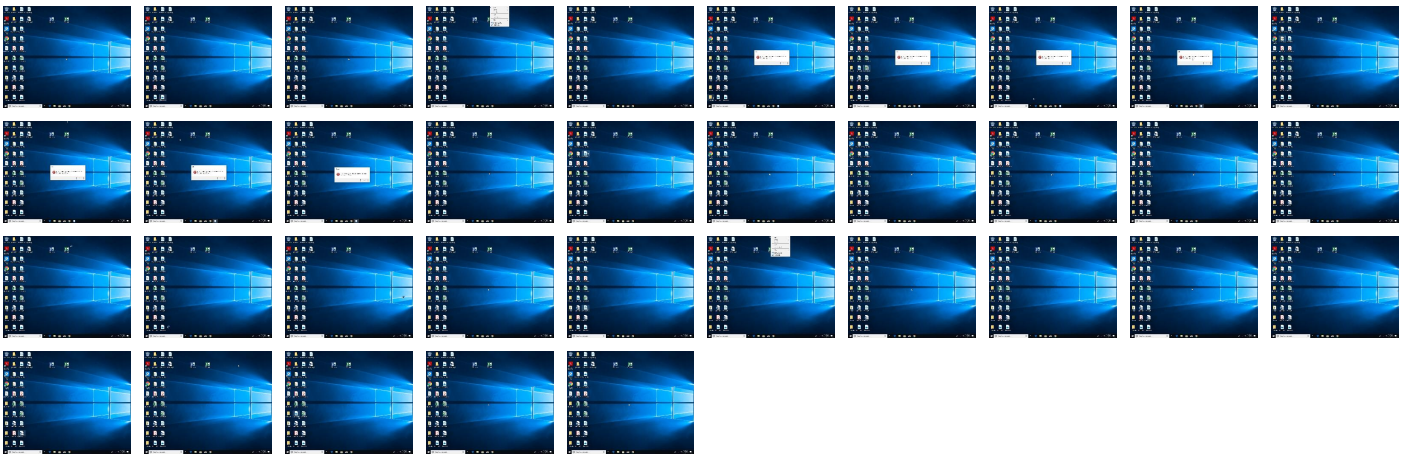
Behavior Graph



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
616412739e268.dll	6%	Virustotal		Browse
616412739e268.dll	24%	ReversingLabs	Win32.Infostealer.Gozi	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.1370000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.0.rundll32.exe.4970000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.4970000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.0.rundll32.exe.4970000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.4cd0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
areuranel.website	7%	Virustotal		Browse
breuranel.website	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=en-us"	0%	Avira URL Cloud	safe	
http://https://watson.tel	0%	Virustotal		Browse
http://https://watson.tel	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
msn.com	13.82.28.61	true	false		high
outlook.com	40.97.116.82	true	false		high
HHN-efz.ms-acdc.office.com	52.97.183.162	true	false		high
FRA-efz.ms-acdc.office.com	52.98.207.194	true	false		high
www.msn.com	unknown	unknown	false		high
www.outlook.com	unknown	unknown	false		high
areuranel.website	unknown	unknown	true	• 7%, Virustotal, Browse	unknown
breuranel.website	unknown	unknown	true	• 7%, Virustotal, Browse	unknown
outlook.office365.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://outlook.com/signup/liopolo/rNcthdwaMuA/zHzDKpXzKq0_2F/hgSdOtaWvkDNGgYpqBLqh/fnirw5AL03xUm4gv/1SKDwhrC85cQhDG/iqhTJ3hi9wsaeKx0vI/xO4E5YLZP/YP9uSugvYABSkowPk9S_/2B24KB1lGZ7pVE71wAB/PNLOy1DTAkJRmo3faOVpWQ/D9BP51I5FAmCi/mjxkDJSf_2B0/dO3cuvbU.jre	false		high
http://https://outlook.com/signup/liopolo/D7_2FrbWNPWoNOhc8CKrYUD/YRyHNJx0fY/hev8f_2BW8cdb94NA/BoQXWWXay0D_/2BZ8Igd1CtC/8Zrwrke0SVrRun/EK5gc9OXOLgsoPgBxCQd1/LxUG0ef0GKyYljGP/_2FJyXjT77_2FZy/ZTRUMkvuvl3KPO1sTr/Mf1qwqvM6/BRuq80kiRu4imCu3Mccr/qTiEDWDGE96/Qopva.jre	false		high
http://https://msn.com/mail/liopolo/NtZggqxIX2EF9w_2/BavTQ0jHk8z72E0/mrA_2BNo5fGf18qS53/GIhA4FNpc/qIQbJVkxLHpIx3LzJcYF/3uQz3PgIC5Pjndy7vBH/i_2FOaoK6pUzqTQ2mVu3pq/cfXt8VkJHx4pF/9i2ySYSz/e6Fwjd_2BYZ5QEKc2Ev8w_2/FX9nTU6mpV/BkgebLJcyW_2BOHak/X7QoD77ir05E/ic.jre	false		high
http://https://outlook.office365.com/signup/liopolo/rNcthdwaMuA/zHzDKpXzKq0_2F/hgSdOtaWvkDNGgYpqBLqh/fnirw5AL03xUm4gv/1SKDwhrC85cQhDG/iqhTJ3hi9wsaeKx0vI/xO4E5YLZP/YP9uSugvYABSkowPk9S_/2B24KB1lGZ7pVE71wAB/PNLOy1DTAkJRmo3faOVpWQ/D9BP51I5FAmCi/mjxkDJSf_2B0/dO3cuvbU.jre	false		high
http://https://msn.com/mail/liopolo/5hHdOh6aVGIiN/xm3v7_2B/EkShunhzAo7MsZ9CmkqFWtX/3z_2Bns4ON/91CWMsZkh9K0L_2FK/DGWBtSEwajEJ/0TtpREbudd5/QgJK102N2T9j48/a7_2B8h2NmEQ_2FO6HINr/eS5x2dWmrnxEuUas/E6VYZyoESNredc4/JUFmKkMiSye_2BBKeH/JexZCfmhU/vSKjW_2B8KOY/RYzBQt1.jre	false		high
http://https://www.outlook.com/signup/liopolo/D7_2FrbWNPWoNOhc8CKrYUD/YRyHNJx0fY/hev8f_2BW8cdb94NA/BoQXWWXay0D_/2BZ8Igd1CtC/8Zrwrke0SVrRun/EK5gc9OXOLgsoPgBxCQd1/LxUG0ef0GKyYljGP/_2FJyXjT77_2FZy/ZTRUMkvuvl3KPO1sTr/Mf1qwqvM6/BRuq80kiRu4imCu3Mccr/qTiEDWDGE96/Qopva.jre	false		high
http://https://www.outlook.com/signup/liopolo/rNcthdwaMuA/zHzDKpXzKq0_2F/hgSdOtaWvkDNGgYpqBLqh/fnirw5AL03xUm4gv/1SKDwhrC85cQhDG/iqhTJ3hi9wsaeKx0vI/xO4E5YLZP/YP9uSugvYABSkowPk9S_/2B24KB1lGZ7pVE71wAB/PNLOy1DTAkJRmo3faOVpWQ/D9BP51I5FAmCi/mjxkDJSf_2B0/dO3cuvbU.jre	false		high
http://https://outlook.office365.com/signup/liopolo/D7_2FrbWNPWoNOhc8CKrYUD/YRyHNJx0fY/hev8f_2BW8cdb94NA/BoQXWWXay0D_/2BZ8Igd1CtC/8Zrwrke0SVrRun/EK5gc9OXOLgsoPgBxCQd1/LxUG0ef0GKyYljGP/_2FJyXjT77_2FZy/ZTRUMkvuvl3KPO1sTr/Mf1qwqvM6/BRuq80kiRu4imCu3Mccr/qTiEDWDGE96/Qopva.jre	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.98.207.194	FRA-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.218.66	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
52.97.218.82	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.101.124.226	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.97.153.146	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
13.82.28.61	msn.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.137.210	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
40.97.116.82	outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.183.162	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	500413
Start date:	12.10.2021
Start time:	00:35:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	616412739e268.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:	27
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:	mal96.troj.evad.winDLL@14/12@24/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18% (good quality ratio 16.9%) • Quality average: 77.6% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 68% • 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 • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:37:39	API Interceptor	8x Sleep call for process: rundll32.exe modified
00:37:49	API Interceptor	8x Sleep call for process: loaddll32.exe modified
00:37:57	API Interceptor	3x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
40.101.124.226	S5.exe	Get hash	malicious	Browse	
40.97.153.146	m87xfb63XU.dll	Get hash	malicious	Browse	
	test1.dll	Get hash	malicious	Browse	
	7.dll	Get hash	malicious	Browse	
	nT5pUwoJSS.dll	Get hash	malicious	Browse	
	5instructio.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	61Documen.exe	Get hash	malicious	Browse	
	65document.exe	Get hash	malicious	Browse	
	29mail98@vip.son.exe	Get hash	malicious	Browse	
	57document.exe	Get hash	malicious	Browse	
13.82.28.61	45DOC001117380115378186353 91-pdf.exe	Get hash	malicious	Browse	• msn.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
outlook.com	P2AN3Yrtnz.exe	Get hash	malicious	Browse	• 40.93.212.0
	Hm7d40tE44.exe	Get hash	malicious	Browse	• 104.47.53.36
	SecuriteInfo.com.W32.AIDetect.malware2.21009.exe	Get hash	malicious	Browse	• 104.47.53.36
	in7BcpKNoa.exe	Get hash	malicious	Browse	• 40.93.212.0
	aXNdDIO708.exe	Get hash	malicious	Browse	• 104.47.53.36
	vhPaw5lCuv.exe	Get hash	malicious	Browse	• 40.93.212.0
	5sTWnI5RoC.exe	Get hash	malicious	Browse	• 40.93.207.0
	57wF9hu0V5.exe	Get hash	malicious	Browse	• 40.93.207.0
	7zxmUw3Ml1.exe	Get hash	malicious	Browse	• 104.47.53.36
	Nh1UI4PFGW.exe	Get hash	malicious	Browse	• 52.101.24.0
	rEYF2xcbGR.exe	Get hash	malicious	Browse	• 40.93.207.1
	G2Shy4flZe.exe	Get hash	malicious	Browse	• 40.93.207.1
	2nqVnWlyLp.exe	Get hash	malicious	Browse	• 52.101.24.0

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	m87xfb63XU.dll	Get hash	malicious	Browse	• 40.101.60.226
	m87xfb63XU.dll	Get hash	malicious	Browse	• 52.97.151.66
	6yDD19jMIu.dll	Get hash	malicious	Browse	• 13.82.28.61
	6yDD19jMIu.dll	Get hash	malicious	Browse	• 13.82.28.61
	B6VQd36tt6.dll	Get hash	malicious	Browse	• 13.82.28.61
	B6VQd36tt6.dll	Get hash	malicious	Browse	• 52.97.183.162
	P2AN3Yrtnz.exe	Get hash	malicious	Browse	• 40.93.212.0
	b3astmode.x86	Get hash	malicious	Browse	• 72.154.237.78
	b3astmode.arm7	Get hash	malicious	Browse	• 20.153.181.154
	b3astmode.arm7-20211011-1850	Get hash	malicious	Browse	• 20.63.129.213

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TNIZtb3HS3.exe	Get hash	malicious	Browse	• 20.42.65.92
	PROFORMA INVOICE -PI6120..html	Get hash	malicious	Browse	• 40.101.62.34
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 52.168.117.173
	ntpclient	Get hash	malicious	Browse	• 21.215.78.72
	2021catalog-selected products.xlsm	Get hash	malicious	Browse	• 13.92.100.208
	K6E9636Koq	Get hash	malicious	Browse	• 159.27.209.248
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 20.42.73.29
	Hm7d40tE44.exe	Get hash	malicious	Browse	• 104.47.53.36
	mixsix_20211008-150045.exe	Get hash	malicious	Browse	• 20.189.173.22
	SecuriteInfo.com.W32.AIDetect.malware2.21009.exe	Get hash	malicious	Browse	• 104.47.53.36
MICROSOFT-CORP-MSN-AS-BLOCKUS	m87xfb63XU.dll	Get hash	malicious	Browse	• 40.101.60.226
	m87xfb63XU.dll	Get hash	malicious	Browse	• 52.97.151.66
	6yDD19jMIu.dll	Get hash	malicious	Browse	• 13.82.28.61
	6yDD19jMIu.dll	Get hash	malicious	Browse	• 13.82.28.61
	B6VQd36tt6.dll	Get hash	malicious	Browse	• 13.82.28.61
	B6VQd36tt6.dll	Get hash	malicious	Browse	• 52.97.183.162
	P2AN3Yrtnz.exe	Get hash	malicious	Browse	• 40.93.212.0
	b3astmode.x86	Get hash	malicious	Browse	• 72.154.237.78
	b3astmode.arm7	Get hash	malicious	Browse	• 20.153.181.154
	b3astmode.arm7-20211011-1850	Get hash	malicious	Browse	• 20.63.129.213
	TNIZtb3HS3.exe	Get hash	malicious	Browse	• 20.42.65.92
	PROFORMA INVOICE -PI6120..html	Get hash	malicious	Browse	• 40.101.62.34
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 52.168.117.173
	ntpclient	Get hash	malicious	Browse	• 21.215.78.72
	2021catalog-selected products.xlsm	Get hash	malicious	Browse	• 13.92.100.208
	K6E9636Koq	Get hash	malicious	Browse	• 159.27.209.248
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 20.42.73.29
	Hm7d40tE44.exe	Get hash	malicious	Browse	• 104.47.53.36
	mixsix_20211008-150045.exe	Get hash	malicious	Browse	• 20.189.173.22
	SecuriteInfo.com.W32.AIDetect.malware2.21009.exe	Get hash	malicious	Browse	• 104.47.53.36

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	m87xfb63XU.dll	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	m87xfb63XU.dll	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	6yDD19jMIu.dll	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	6yDD19jMIu.dll	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	B6VQd36tt6.dll	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	B6VQd36tt6.dll	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	aVFOmbW2t7.dll	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	gxJ83rJkgw.msi	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	yR4AxlwcWJ.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	BsyK7FB5DQ.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	SGfGZT66wD.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	uT9rwkGATJ.dll	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	XK1PLPuwjL.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	pHEiqE9toa.msi	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	SecuriteInfo.com.W32.AIDetect.malware2.24481.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	vH0SHswvrb.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	NM0NyvZi8O.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	yOTzv1Qz0n.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162
	SWaTAV7EdD.exe	Get hash	malicious	Browse	• 52.97.218.82 • 40.101.124.226 • 40.97.153.146 • 52.98.207.194 • 52.97.218.66 • 13.82.28.61 • 52.97.137.210 • 40.97.116.82 • 52.97.183.162

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_d4e7795f79114aeb9c4dc9cc69e25e6282339_82810a17_1874b820\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12044
Entropy (8bit):	3.765368455363511

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_d4e7795f79114aeb9c4dc9cc69e25e6282339_82810a17_1874b820\Report.wer

Encrypted:	false
SSDEEP:	192:0YuiJ0oXAHBUZMX4jed+x/u7sAwS274It7cJ:MinXoBUZMX4je8/u7sAwX4It7cJ
MD5:	316CE6E876A182906C00DD2AD8F35040
SHA1:	54AD11020F6730D0C756C5682E1BAEA55AE1F317
SHA-256:	74EA72682FCB32B1165308196313E62BADE799EF2947E6D132D5A0D077219B19
SHA-512:	749DD024BDC05C4918700FCF5740173D68F7FCEF20A4C56BCFF2D894123A628A78AF6B8103512056FBBEF378828B4AAEA3F757FA297DF91C155835C7FD19E77(
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.8.4.6.5.4.6.8.2.6.1.5.0.0.8.....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.=.1.3.2.7.8.4.6.5.4.7.5.6.0.5.2.3.9.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.6.5.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.0.2.d.3.f.3.5.-.4.3.8.7.-.4.f.e.d.-.b.7.a.f.-.7.6.8.4.9.9.3.f.7.a.9.9.....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.=.8.d.0.4.5.a.6.7.-.2.2.2.e.-.4.c.7.2.-.b.b.e.c.-.0.8.9.b.4.0.8.1.c.f.f.9.....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.=.0.0.0.0.1.b.a.0.-.0.0.0.1.-.0.0.1.b.-.d.a.8.9.-.2.e.6.0.f.0.b.e.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.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_d4e7795f79114aeb9c4dc9cc69e25e6282339_82810a17_19a08827\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12246
Entropy (8bit):	3.765114618947458
Encrypted:	false
SSDEEP:	192:ogaPiW0oX7HBUZMX4jed+j/u7sSS274It7cl:oJPiQXbBUZMX4jeO/u7sSX4It7cl
MD5:	9CF8099E09C39847EFFF6FB7B70CEA33
SHA1:	16B081768605B3C60E9DBF23A1646EBDF70337E0
SHA-256:	D780C3F704283D57B71AE6362A0F6095E72DEDC4D08062E15094DF7FA1DAD471
SHA-512:	F9873C535120F8E9BEF91F26B93B9251BD6F06F506E7D53E5EDDAE3E23AE04674686E39BD8BB186632AFF0A43717117E4F61818502AE49E938D546F5FA34EE37
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.8.4.6.5.4.7.9.9.9.8.3.1.7.3.....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.=.1.3.2.7.8.4.6.5.4.9.3.9.0.4.4.8.4.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.6.5.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.d.1.d.e.5.4.7.-.b.d.c.0.-.4.a.7.4.-.9.0.f.e.-.4.f.e.1.f.8.d.b.f.f.b.b.....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.b.e.9.a.1.f.8.-.8.2.c.a.-.4.a.c.0.-.9.c.1.f.-.0.4.d.d.4.9.8.8.b.9.8.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.=.0.0.0.0.1.9.4.0.-.0.0.0.1.-.0.0.1.b.-.f.8.7.1.-.3.6.6.7.f.0.b.e.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.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_d4e7795f79114aeb9c4dc9cc69e25e6282339_82810a17_1be8e7ac\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12040
Entropy (8bit):	3.7654289890935924
Encrypted:	false
SSDEEP:	192:43iu0oX/HBUZMX4jed+x/u7sAwS274It7c/V:IiYX/BUZMX4je8/u7sAwX4It7c/V
MD5:	47234B5A061C3D57518C75D012598E15
SHA1:	8054E955AA6274E52832CECAC7BF98AB2AAC4A3E
SHA-256:	BF44ADFD50F9CC39C25CC5B4642FD4EE5C007226F9AEDC5BBCA7FBA5DDBF6E4F
SHA-512:	273E8DA585B81F6C6468E2BFFE4E452420D55F06597B6BE6F59747DB2FB96326B7C015A610D4D5A5B1F663593E3398E04C118600B7A5838156B1A568928CE7C6
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.8.4.6.5.4.7.5.0.8.9.8.8.9.3.....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.=.1.3.2.7.8.4.6.5.4.8.8.7.3.0.5.2.7.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.6.5.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.4.9.5.e.6.6.3.-.8.9.1.b.-.4.5.3.4.-.a.c.6.0.-.b.9.b.2.2.c.2.8.0.c.a.8.....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.=.3.e.a.7.1.d.2.7.-.d.c.2.f.-.4.e.0.1.-.a.e.c.e.-.3.b.4.9.0.b.5.1.3.6.2.2.....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.=.0.0.0.0.0.5.5.4.-.0.0.0.1.-.0.0.1.b.-.2.7.a.b.-.4.b.6.2.f.0.b.e.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.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EDD.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Oct 11 22:37:50 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	35838
Entropy (8bit):	2.3956337648230916
Encrypted:	false
SSDEEP:	192:zRpsH1iJ4InP5sfRuvUM+sOI36GDZ69CA4nxZN5knmhpIRY:dCkiInERYN+i6G0s1nF5kmc2
MD5:	6314F249ADC86966FA67E57AE5C44922
SHA1:	FFCAA1E89BAD579997BE419D71AA5F670200CD69

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EDD.tmp.dmp	
SHA-256:	39A76F75342336856B50BBC0B977FBE57722A50B0BD0008499FBBC2A0B263C10
SHA-512:	95B2148C5D3E31169DD1EBF64FACE7B4728DB4473EA9EC225A992B4BFD640E8E9C29393C9BDE50C99E9EAA94FB45EAA11BECFCC3CF2DE1063EDA9ACA9EA0 2DBB
Malicious:	false
Preview:	MDMP..... .....da.....U.....B.....GenuineIntelW.....T.....T.da".....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... .E.u.r.o.p.e. .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\WER270C.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):	8404
Entropy (8bit):	3.698373923142492
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/j/6ZCy6YoDz6Tofg4dgmf8zSNz+prz89bDdsf0Bm:RrlsNiL/6oy6YCz6Tofg4dgmf8zSNjDk
MD5:	D9504C279DAD3BB36B90B2ABB8BD6024
SHA1:	8F897066FFB317B3CB6FE7CEDDCD657ABEFA0AD2
SHA-256:	10A8657425ED12843DE5D88E4AC5FB228E04E30FC2285B5ABFAB0644D4F5FDED
SHA-512:	1E599A129E128BDA89BBD6B4D4EBB20D56F4B4C3576399CFAF5B5EA8B4227ECE0156F047B9B628EA4091B4D3D829501B68118A87EA09EC46B4ECCE0E714F16 F8
Malicious:	false
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.>.7.0.7.2.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER29CC.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.4859311182693515
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdNJgtWI9jZVWSC8B2+8fm8M4JCdsTMF3+q8vjsTJO4SrSWd:uITf9EqSN07JNmKiJODWWd
MD5:	14148F5D29C531D9A2DAB8BE378319B4
SHA1:	2555ADA459F857D0F04C818ED0FA3523FBAEDA54
SHA-256:	345133599386F0C3CD20ADF62510BA963E25DC1EE938691229F2E011F02CCF15
SHA-512:	FDC853B50B28C8C90540AB31EBB67DE00BA0BEBE28A69CE469CCECE120487E62648DBF600DFC5F3F58211436306E7276FB12B579879897A84E1DD82E612446E 0
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="1205748" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER398A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Oct 11 22:37:57 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	34760
Entropy (8bit):	2.413605188260289
Encrypted:	false
SSDEEP:	192:NICEknpSR00ugBtrvUM+sOI36FDZuzLNR2GK0KHnIZ1S1:PEPTN+i6FknX2GQIZ1C
MD5:	FE3A9A57895A11BBDE379864BD34A1AA
SHA1:	4660CCA0FFEDA2D9F0CC371B0E756BEBEE1E59CA
SHA-256:	D3DAFB26C47511DD9A99713F077D9D3503749D9A128772ED3BCE2381FAD98C2B
SHA-512:	5BF3A8825B1CBFB3F54916D2BE008CEC447763A16AB6A130FD3A78496E6D3DB5C9239FCEF211919354E6B78A3070072128C6A646F42403F0935A44ADB14B951E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER398A.tmp.dmp	
Preview:	MDMP..... .....da.....U.....B.....GenuineIntelW.....T.....T...X.da!.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WER4543.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):	8412
Entropy (8bit):	3.6972167795220234
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiV36p6Yo76njOxp2+Pgmf8zSNz+pry89bLFsflZm:RrlsNiF6p6YU6axp2+Pgmf8zSNcLefy
MD5:	76872B4F10DAB5548F7C5A90D51D5856
SHA1:	09F65EB354956B8BDF85D560CB00855480EDA67B
SHA-256:	7590A90E442F73573110BB00A58EC1D1B8B6E6A7F8C43CA37ECB25682A052922
SHA-512:	8E63F1986DE67951325919E86C1A72F463AAD58723FE2E3710743EC271304908CF6D0C12B2CF3E2C6AF141782DC7BF36C68EC556A88DC3E01F000761D828CFC
Malicious:	false
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.>.1.3.6.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A83.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.486599306136513
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdNJgtWI9jZVWSC8B2r8fm8M4JCdsTMFl+q8vjsTh4SrSh6d:uITf9EqSN0IJNoKihDWh6d
MD5:	F5119CC37CD940B95701B555B8405D56
SHA1:	0F6AEC842D402C511BC033B95CDDE4B721F845CA
SHA-256:	7B59F212C271180A12BD3B2F239E245B604E7BE9F2F6D4BDD729106A8E0E63E5
SHA-512:	CAF3A254182B3FA64D7552562B9144A51D49A778C28225E64364D84C9B46F065861BF8E23F693BBCA769AB0D02137C69AB3B75B120D2C2582A245C0804917952
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="1205748" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER4CB4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Oct 11 22:38:06 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	36016
Entropy (8bit):	2.4897777598497166
Encrypted:	false
SSDEEP:	192:xC0HXLDCwswpbRb3TZO2ODjUyrcFl7yuQM8BXEZniQcd9eq:s0771b1WUyrcPSM8Biinyq
MD5:	559FD5E2D54239F3AF7994402E1F225A
SHA1:	6F975E163EC0244D6973DCF1058DC318A990BAAF
SHA-256:	4E9B64C1A7891E3469C235B9E4F92693B6D9451B09FE8BB64D09FA8CFDA9EF47
SHA-512:	B03EA1DB6B58C4DFCD6BACEBC95BFD282F11D8BE9DF5F0ECF7F32F958898832D290CD6ED3B21D6D8A40C201D81B71625C0E6F27C670708CF7536212D02B6BAB
Malicious:	false
Preview:	MDMP..... .....da.....U.....B.....GenuineIntelW.....T.....@...`.da!.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WER6984.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):	8416
Entropy (8bit):	3.697753685979791
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi926o6jYy6Yoy6xgmf8zSNz+prfZ89bYbasfyejm:RrlsNis6o6jYy6Y96xgmf8zSNpYb5fL6
MD5:	BADE93E59CD5720AB99E2508033FE2BB
SHA1:	9257D92BE814163ED9D6E71DC5F282D0377CD90D
SHA-256:	E0576D35FA22FA6525FED18862A5C4D3FEF0A7DDA9ABA2DD711D994276920D3C
SHA-512:	5A8B6AE760691632CBF5B4D45DC7E9DDBA241701D9C2D018A106BB338FCCA751E73FCF7FC789E9AD8C4745FA6D464E7050176AC96293F752BA48C24A4042FF 7
Malicious:	false
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.>.6.4.6.4.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E67.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.486306505900062
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdNJgtWI9jZVWSC8B2Q8fm8M4JCdsTMFMDGv+q8vjsTv4SrSld:uITf9EqSN0tJNYvKivDWld
MD5:	139252536DD735CAA02910CCEF45FF77
SHA1:	B5EA76ED280C8826367FF09C33596FBD7E73E301
SHA-256:	D78ACA3358C19DB67E52384ED6AEE82B755A321E0E5963312DBDE4B5DFD8C370
SHA-512:	5BC27230DB2D3272AD98C0DFE3BB0BA29425ED587B6909065F635691F54F9B0A282092D6970FA70DD72D9A93ADAA3CD7691B1604ADD93176B25CCAEA6EF0EA 9
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="1205748" />.. <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" />..

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	6.669952151971332
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	616412739e268.dll
File size:	718336
MD5:	9e67e68ddbedba865b91b5469ab642ef
SHA1:	f2c7b0735343081be06e48616d0fc14235a28744
SHA256:	41c0934ba1be030dbae45893107f6a2ae5f99c79d763462 6263cdf809f7556ee
SHA512:	802d983ca7ca04ae737da69ed5772eece8f408c6c02c8d 0c42cfea1c1abf25236b02c35c09d56f3ba6a229b3b71f7 2fa3d4c6735c8670c76affdbbc139b63d87
SSDEEP:	12288:aUAQSxl6fDEr8Np6b/rPPsjosrS9aEoe+0JCym+ 4YJAOSVUNcuHIGF4uW/XrGAsV:az3xl6fq8Np6bTPPa BreaZlYCOSVol2a

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m$aV.J2V.J2V.J2...2U.J2_t.2H.J2.cH3R.J2.cO3_.J2.cI3D.J2...2H.J2V.K2..J2.cO3).J2.cJ3W.J2.cJ3W.J2V..2W.J2.cH3W.J2RichV.J2.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1003ab77
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F700BB2 [Sun Sep 27 03:49:06 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	b5c6badd398e2e3aa283a40a40432c6c

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x79f71	0x7a000	False	0.510071801358	data	6.75463290974	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7b000	0x2e586	0x2e600	False	0.556366871631	data	5.60181106954	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xaa000	0x9b19c	0x1800	False	0.190266927083	data	4.15778005426	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x146000	0x53d0	0x5400	False	0.752650669643	data	6.72453697464	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 12, 2021 00:38:03.208512068 CEST	192.168.2.4	8.8.8.8	0x8ef2	Standard query (0)	msn.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:05.070362091 CEST	192.168.2.4	8.8.8.8	0xc63a	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:10.907257080 CEST	192.168.2.4	8.8.8.8	0x9600	Standard query (0)	msn.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:11.716469049 CEST	192.168.2.4	8.8.8.8	0xf4cf	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:25.800733089 CEST	192.168.2.4	8.8.8.8	0x9f0c	Standard query (0)	breuranel.website	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:32.527570009 CEST	192.168.2.4	8.8.8.8	0xe0e2	Standard query (0)	breuranel.website	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.880023956 CEST	192.168.2.4	8.8.8.8	0x9608	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.614259958 CEST	192.168.2.4	8.8.8.8	0x77ee	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.775543928 CEST	192.168.2.4	8.8.8.8	0x8150	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:52.743369102 CEST	192.168.2.4	8.8.8.8	0x6526	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.220117092 CEST	192.168.2.4	8.8.8.8	0x211d	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.397085905 CEST	192.168.2.4	8.8.8.8	0x4078	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:07.148479939 CEST	192.168.2.4	8.8.8.8	0xca44	Standard query (0)	areuranel.website	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:13.816450119 CEST	192.168.2.4	8.8.8.8	0x8a5	Standard query (0)	areuranel.website	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:27.242336988 CEST	192.168.2.4	8.8.8.8	0x7db	Standard query (0)	msn.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:27.719876051 CEST	192.168.2.4	8.8.8.8	0xf46f	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:33.981678963 CEST	192.168.2.4	8.8.8.8	0xb117	Standard query (0)	msn.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:34.465598106 CEST	192.168.2.4	8.8.8.8	0x128d	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:48.098314047 CEST	192.168.2.4	8.8.8.8	0x2804	Standard query (0)	breuranel.website	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:55.946903944 CEST	192.168.2.4	8.8.8.8	0x8958	Standard query (0)	breuranel.website	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.155658960 CEST	192.168.2.4	8.8.8.8	0xf83	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.626851082 CEST	192.168.2.4	8.8.8.8	0x901e	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.775460958 CEST	192.168.2.4	8.8.8.8	0x1deb	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:15.993360043 CEST	192.168.2.4	8.8.8.8	0x8b0c	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 00:38:03.228565931 CEST	8.8.8.8	192.168.2.4	0x8ef2	No error (0)	msn.com		13.82.28.61	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:05.088568926 CEST	8.8.8.8	192.168.2.4	0xc63a	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:10.925432920 CEST	8.8.8.8	192.168.2.4	0x9600	No error (0)	msn.com		13.82.28.61	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:11.734641075 CEST	8.8.8.8	192.168.2.4	0xf4cf	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:25.818322897 CEST	8.8.8.8	192.168.2.4	0x9f0c	Name error (3)	breuranel.website	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 00:38:32.546330929 CEST	8.8.8.8	192.168.2.4	0xe0e2	Name error (3)	breuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.897805929 CEST	8.8.8.8	192.168.2.4	0x9608	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.897805929 CEST	8.8.8.8	192.168.2.4	0x9608	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.897805929 CEST	8.8.8.8	192.168.2.4	0x9608	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.897805929 CEST	8.8.8.8	192.168.2.4	0x9608	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.897805929 CEST	8.8.8.8	192.168.2.4	0x9608	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.897805929 CEST	8.8.8.8	192.168.2.4	0x9608	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.897805929 CEST	8.8.8.8	192.168.2.4	0x9608	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:45.897805929 CEST	8.8.8.8	192.168.2.4	0x9608	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.632378101 CEST	8.8.8.8	192.168.2.4	0x77ee	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:46.632378101 CEST	8.8.8.8	192.168.2.4	0x77ee	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:46.632378101 CEST	8.8.8.8	192.168.2.4	0x77ee	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:46.632378101 CEST	8.8.8.8	192.168.2.4	0x77ee	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:46.632378101 CEST	8.8.8.8	192.168.2.4	0x77ee	No error (0)	HHN-efz.ms-acdc.office.com		52.97.183.162	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.632378101 CEST	8.8.8.8	192.168.2.4	0x77ee	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.98	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.632378101 CEST	8.8.8.8	192.168.2.4	0x77ee	No error (0)	HHN-efz.ms-acdc.office.com		52.97.178.98	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.632378101 CEST	8.8.8.8	192.168.2.4	0x77ee	No error (0)	HHN-efz.ms-acdc.office.com		52.97.223.66	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.794441938 CEST	8.8.8.8	192.168.2.4	0x8150	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:46.794441938 CEST	8.8.8.8	192.168.2.4	0x8150	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:46.794441938 CEST	8.8.8.8	192.168.2.4	0x8150	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:46.794441938 CEST	8.8.8.8	192.168.2.4	0x8150	No error (0)	HHN-efz.ms-acdc.office.com		52.97.218.82	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.794441938 CEST	8.8.8.8	192.168.2.4	0x8150	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.130	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.794441938 CEST	8.8.8.8	192.168.2.4	0x8150	No error (0)	HHN-efz.ms-acdc.office.com		52.97.219.162	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:46.794441938 CEST	8.8.8.8	192.168.2.4	0x8150	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.242	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:52.760597944 CEST	8.8.8.8	192.168.2.4	0x6526	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:52.760597944 CEST	8.8.8.8	192.168.2.4	0x6526	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 00:38:52.760597944 CEST	8.8.8.8	192.168.2.4	0x6526	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:52.760597944 CEST	8.8.8.8	192.168.2.4	0x6526	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:52.760597944 CEST	8.8.8.8	192.168.2.4	0x6526	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:52.760597944 CEST	8.8.8.8	192.168.2.4	0x6526	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:52.760597944 CEST	8.8.8.8	192.168.2.4	0x6526	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:52.760597944 CEST	8.8.8.8	192.168.2.4	0x6526	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.240650892 CEST	8.8.8.8	192.168.2.4	0x211d	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:53.240650892 CEST	8.8.8.8	192.168.2.4	0x211d	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:53.240650892 CEST	8.8.8.8	192.168.2.4	0x211d	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:53.240650892 CEST	8.8.8.8	192.168.2.4	0x211d	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:53.240650892 CEST	8.8.8.8	192.168.2.4	0x211d	No error (0)	HHN-efz.ms-acdc.office.com		52.97.218.66	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.240650892 CEST	8.8.8.8	192.168.2.4	0x211d	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.146	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.240650892 CEST	8.8.8.8	192.168.2.4	0x211d	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.2	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.240650892 CEST	8.8.8.8	192.168.2.4	0x211d	No error (0)	HHN-efz.ms-acdc.office.com		52.98.208.50	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.415934086 CEST	8.8.8.8	192.168.2.4	0x4078	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:53.415934086 CEST	8.8.8.8	192.168.2.4	0x4078	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:53.415934086 CEST	8.8.8.8	192.168.2.4	0x4078	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:38:53.415934086 CEST	8.8.8.8	192.168.2.4	0x4078	No error (0)	HHN-efz.ms-acdc.office.com		52.97.137.210	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.415934086 CEST	8.8.8.8	192.168.2.4	0x4078	No error (0)	HHN-efz.ms-acdc.office.com		52.98.199.194	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.415934086 CEST	8.8.8.8	192.168.2.4	0x4078	No error (0)	HHN-efz.ms-acdc.office.com		52.98.223.162	A (IP address)	IN (0x0001)
Oct 12, 2021 00:38:53.415934086 CEST	8.8.8.8	192.168.2.4	0x4078	No error (0)	HHN-efz.ms-acdc.office.com		52.97.171.194	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:07.172518015 CEST	8.8.8.8	192.168.2.4	0xca44	Name error (3)	areuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:13.840886116 CEST	8.8.8.8	192.168.2.4	0x8a5	Name error (3)	areuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:27.260047913 CEST	8.8.8.8	192.168.2.4	0x7db	No error (0)	msn.com		13.82.28.61	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:27.740092039 CEST	8.8.8.8	192.168.2.4	0xf46f	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:39:34.002629995 CEST	8.8.8.8	192.168.2.4	0xb117	No error (0)	msn.com		13.82.28.61	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 00:39:34.485994101 CEST	8.8.8.8	192.168.2.4	0x128d	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:39:48.117002010 CEST	8.8.8.8	192.168.2.4	0x2804	Name error (3)	breuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 00:39:55.966435909 CEST	8.8.8.8	192.168.2.4	0x8958	Name error (3)	breuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.176791906 CEST	8.8.8.8	192.168.2.4	0xf83	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.176791906 CEST	8.8.8.8	192.168.2.4	0xf83	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.176791906 CEST	8.8.8.8	192.168.2.4	0xf83	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.176791906 CEST	8.8.8.8	192.168.2.4	0xf83	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.176791906 CEST	8.8.8.8	192.168.2.4	0xf83	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.176791906 CEST	8.8.8.8	192.168.2.4	0xf83	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.176791906 CEST	8.8.8.8	192.168.2.4	0xf83	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.176791906 CEST	8.8.8.8	192.168.2.4	0xf83	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.644534111 CEST	8.8.8.8	192.168.2.4	0x901e	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:40:08.644534111 CEST	8.8.8.8	192.168.2.4	0x901e	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:40:08.644534111 CEST	8.8.8.8	192.168.2.4	0x901e	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:40:08.644534111 CEST	8.8.8.8	192.168.2.4	0x901e	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:40:08.644534111 CEST	8.8.8.8	192.168.2.4	0x901e	No error (0)	FRA-efz.ms-acdc.office.com		52.98.207.194	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.644534111 CEST	8.8.8.8	192.168.2.4	0x901e	No error (0)	FRA-efz.ms-acdc.office.com		52.98.208.34	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.644534111 CEST	8.8.8.8	192.168.2.4	0x901e	No error (0)	FRA-efz.ms-acdc.office.com		52.98.208.50	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.795043945 CEST	8.8.8.8	192.168.2.4	0x1deb	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:40:08.795043945 CEST	8.8.8.8	192.168.2.4	0x1deb	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:40:08.795043945 CEST	8.8.8.8	192.168.2.4	0x1deb	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 12, 2021 00:40:08.795043945 CEST	8.8.8.8	192.168.2.4	0x1deb	No error (0)	FRA-efz.ms-acdc.office.com		40.101.124.226	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.795043945 CEST	8.8.8.8	192.168.2.4	0x1deb	No error (0)	FRA-efz.ms-acdc.office.com		40.101.124.2	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:08.795043945 CEST	8.8.8.8	192.168.2.4	0x1deb	No error (0)	FRA-efz.ms-acdc.office.com		40.101.9.178	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:16.011079073 CEST	8.8.8.8	192.168.2.4	0x8b0c	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:16.011079073 CEST	8.8.8.8	192.168.2.4	0x8b0c	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 00:40:16.011079073 CEST	8.8.8.8	192.168.2.4	0x8b0c	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:16.011079073 CEST	8.8.8.8	192.168.2.4	0x8b0c	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:16.011079073 CEST	8.8.8.8	192.168.2.4	0x8b0c	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:16.011079073 CEST	8.8.8.8	192.168.2.4	0x8b0c	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:16.011079073 CEST	8.8.8.8	192.168.2.4	0x8b0c	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 12, 2021 00:40:16.011079073 CEST	8.8.8.8	192.168.2.4	0x8b0c	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- msn.com
- outlook.com
- www.outlook.com
- outlook.office365.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49776	13.82.28.61	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:04 UTC	0	OUT	GET /mail/liopolo/31Pla_2BCXtei/1R_2BY6O/xV8Y0PePoExsKvdRsArLjMT/0HY9ewGl4d/RTh7V4sy0BSH_2Btl/9sqK23pzW1xY/kPT6lmvGYLw/Cf2IOR2fhZTyNL/tKZ289_2FYjlbDZolDbOl/xXcWSCD6lIQGRdIS/84EeVY8JQpYoU7N/sMotozvUSzPLgYoFpN/L9urq8t4YJmiCxPtVCV/XUD.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: msn.com
2021-10-11 22:38:04 UTC	0	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.msn.com/mail/liopolo/31Pla_2BCXtei/1R_2BY6O/xV8Y0PePoExsKvdRsArLjMT/0HY9ewGl4d/RTh7V4sy0BSH_2Btl/9sqK23pzW1xY/kPT6lmvGYLw/Cf2IOR2fhZTyNL/tKZ289_2FYjlbDZolDbOl/xXcWSCD6lIQGRdIS/84EeVY8JQpYoU7N/sMotozvUSzPLgYoFpN/L9urq8t4YJmiCxPtVCV/XUD.jre Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Date: Mon, 11 Oct 2021 22:38:04 GMT Connection: close Content-Length: 373
2021-10-11 22:38:04 UTC	0	IN	Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 73 6e 2e 63 6f 6d 2f 6d 61 69 6c 2f 6c 69 6f 70 6f 6c 6f 2f 33 31 50 6c 61 5f 32 42 43 58 74 65 69 2f 31 52 5f 32 42 59 36 4f 2f 78 56 38 59 30 50 65 50 6f 45 78 73 4b 76 64 52 73 41 72 4c 6a 4d 54 2f 30 48 59 39 65 77 47 6c 34 64 2f 52 54 68 37 56 34 73 79 30 42 53 48 5f 32 42 74 6c 2f 39 73 71 4b 32 33 70 7a 57 31 78 59 2f 6b 50 54 36 6c 6d 76 47 59 4c 77 2f 43 66 32 49 4f 52 32 66 68 5a 54 79 4e 4c 2f Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.msn.com/mail/liopolo/31Pla_2BCXtei/1R_2BY6O/xV8Y0PePoExsKvdRsArLjMT/0HY9ewGl4d/RTh7V4sy0BSH_2Btl/9sqK23pzW1xY/kPT6lmvGYLw/Cf2IOR2fhZTyNL/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49779	13.82.28.61	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:11 UTC	1	OUT	GET /mail/liopolo/NtZggqxIX2EF9w_2/BavTQ0jHk8z72E0/mrA_2BNo5fGf18qS53/GIhA4FNpc/qIQbJVkxLHpIx3LzJcYF /3uQz3PgIC5Pjndy7vBH/i_2FOaoK6pUzqTQ2mVu3pq/cfXt8VkJHx4pF/9i2ySYSz/e6Fwjd_2BYZ5QEKc2Ev8w_2 /FX9nTU6mpV/BkgebLJcyW_2BOHak/X7QoD77ir05E/ic.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: msn.com
2021-10-11 22:38:11 UTC	1	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.msn.com/mail/liopolo/NtZggqxIX2EF9w_2/BavTQ0jHk8z72E0/mrA_2BNo5fGf18qS53/GIhA4 FNpc/qIQbJVkxLHpIx3LzJcYF/3uQz3PgIC5Pjndy7vBH/i_2FOaoK6pUzqTQ2mVu3pq/cfXt8VkJHx4pF/9i2ySYSz/e6Fwjd_2 BYZ5QEKc2Ev8w_2/FX9nTU6mpV/BkgebLJcyW_2BOHak/X7QoD77ir05E/ic.jre Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Date: Mon, 11 Oct 2021 22:38:11 GMT Connection: close Content-Length: 377
2021-10-11 22:38:11 UTC	2	IN	Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 73 6e 2e 63 6f 6d 2f 6d 61 69 6c 2f 6c 69 6f 70 6f 6c 6f 2f 4e 74 5a 67 67 71 78 49 58 32 45 46 39 77 5f 32 2f 42 61 76 54 51 30 6a 48 6b 38 7a 37 32 45 30 2f 6d 72 41 5f 32 42 4e 6f 35 66 47 66 31 38 71 53 35 33 2f 47 49 68 41 34 46 4e 70 63 2f 71 49 51 62 4a 56 6b 78 4c 48 70 49 78 33 4c 7a 4a 63 59 46 2f 33 75 51 7a 33 50 67 49 43 35 50 6a 6e 64 79 37 76 42 48 2f 69 5f 32 46 4f 61 6f 4b 36 70 55 7a 71 Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.msn.com/mail/liopolo/NtZggqxIX2EF9w_2/BavTQ0jHk8z72E0/mrA_2BNo5fGf18qS53/GIhA4FNp c/qIQbJVkxLHpIx3LzJcYF/3uQz3PgIC5Pjndy7vBH/i_2FOaoK6pUzq

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49860	40.97.153.146	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:40:08 UTC	14	OUT	GET /signup/liopolo/dtrpOPrEQ8_2/BH4GVvmMwLv/x_2BNp_2Bcq8rr/i2sFrcRmTMjCNusY3oN7V/abYuA7gYAEh57Xzf/m KvjzhmwoOoocH6/Rx6Zaylm3INx2PjsYP/5tKNcBaCE/Tau2dKL_2B3XpLMrimMx/fEyRGxrtqJjdxkKHFLZ/nn7M4 Qsmv3PPoTapEVJO6K/P8DaDVIqQXr3N/9BeM5e5l/i_2F.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com
2021-10-11 22:40:08 UTC	14	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/signup/liopolo/dtrpOPrEQ8_2/BH4GVvmMwLv/x_2BNp_2Bcq8rr/i2sFrcRmTMj CNusY3oN7V/abYuA7gYAEh57Xzf/mKvjzhmwoOoocH6/Rx6Zaylm3INx2PjsYP/5tKNcBaCE/Tau2dKL_2B3XpLMri mMx/fEyRGxrtqJjdxkKHFLZ/nn7M4Qsmv3PPoTapEVJO6K/P8DaDVIqQXr3N/9BeM5e5l/i_2F.jre Server: Microsoft-IIS/10.0 request-id: 448417ac-9aed-bf6f-b902-bf5f92a7f6fb Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: BN6PR2001CA0022 X-RequestId: 0a3dbc15-af9f-42a8-9d5e-2a0de062e8b5 MS-CV: rBeERO2ab7+5Ar9fkqf2+w.0 X-Powered-By: ASP.NET X-FEServer: BN6PR2001CA0022 Date: Mon, 11 Oct 2021 22:40:08 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49861	52.98.207.194	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:40:08 UTC	15	OUT	GET /signup/liopolo/dtrpOPrEQ8_2/BH4GVvmMwLv/x_2BNp_2Bcq8rr/i2sFrcRmTMjCNusY3oN7V/abYuA7gYAEh57Xzf/m KvjzhmwoOoocH6/Rx6Zaylm3INx2PjsYP/5tKNcBaCE/Tau2dKL_2B3XpLMrimMx/fEyRGxrtqJjdxkKHFLZ/nn7M4 Qsmv3PPoTapEVJO6K/P8DaDVIqQXr3N/9BeM5e5l/i_2F.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: www.outlook.com

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:40:08 UTC	15	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/signup/liopolo/dtrpOPrEQ8_2/BH4GVvmMwLv/x_2BNp_2Bcq8rr/i2sFr cRmTMjCNusY3oN7V/abYuA7gYAEh57Xzf/mKvjzhmwo0oocH6/Rx6Zaylm3INx2PjsYP/5tKNcBaCE/Tau2dKL_2B3 XpLMrimMx/fEyRGxrtqJjdxkKHFLZ/nn7M4Qsmv3PPoTapEVJO6K/P8DaDVIqQXr3N/9BeM5e5l/i_2F.jre Server: Microsoft-IIS/10.0 request-id: 6f503dd6-681b-92e6-0e33-05fdd79ea39d Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AS9PR0301CA0009 X-RequestId: 5f53b19c-6d27-4c9c-b051-e6d331879eab MS-CV: 1j1Qbxto5pIOMwX9156jnQ.0 X-Powered-By: ASP.NET X-FEServer: AS9PR0301CA0009 Date: Mon, 11 Oct 2021 22:40:08 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49862	40.101.124.226	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:40:08 UTC	16	OUT	GET /signup/liopolo/dtrpOPrEQ8_2/BH4GVvmMwLv/x_2BNp_2Bcq8rr/i2sFrcRmTMjCNusY3oN7V/abYuA7gYAEh57Xzf/m Kvjzhmwo0oocH6/Rx6Zaylm3INx2PjsYP/5tKNcBaCE/Tau2dKL_2B3XpLMrimMx/fEyRGxrtqJjdxkKHFLZ/nn7M4 Qsmv3PPoTapEVJO6K/P8DaDVIqQXr3N/9BeM5e5l/i_2F.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.office365.com
2021-10-11 22:40:08 UTC	16	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: bd6df30b-3506-0654-39aa-09111fc341ce Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Alt-Svc: h3=":443",h3-29=":443" X-CalculatedFETarget: VI1PR07CU008.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: VI1PR07CA0252.EURPRD07.PROD.OUTLOOK.COM X-CalculatedBETarget: VI1PR01MB6621.EURPRD01.PROD.EXCHANGELABS.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: C/NtvQY1VAY5qgkRH8NBzg.1.1 X-FEServer: VI1PR07CA0252 X-Powered-By: ASP.NET X-FEServer: AM5PR0101CA0012 Date: Mon, 11 Oct 2021 22:40:08 GMT Connection: close
2021-10-11 22:40:08 UTC	17	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49806	40.97.116.82	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:46 UTC	2	OUT	GET /signup/liopolo/D7_2FrbWNPWoNOhc8CKrYUD/YRyHNJx0fY/hev8f_2BW8cdb94NA/BoQXWWXay0D_/2BZ8 lgd1CtC/8Zrwrke0SVrRun/EK5gc9OXOLgsoPgBxCQd1/LxUG0ef0GKyYljGP/_2FJyXjT77_2FZy/ZTRUMkvuvl3K PO1sTr/Mf1qwqvM6/BRuq80kiRu4imCu3Mccr/qTiEDWDGE96/Qopva.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:46 UTC	2	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/signup/liopolo/D7_2FrbWNPWoNOhc8CKrYUD/YRyHNJx0fY/hev8f_2BW8cdb94N A/BoQXWWXay0D_/2BZ8Igd1CtC/8Zrwrke0SVrRun/EK5gc9OXOLgsoPgBxCQd1/LxUG0ef0GKyYljGP/_2FJyXjT7 7_2FZy/ZTRUMkvuvl3KPO1sTr/Mf1qwqvM6/BRuq80kiRu4imCu3Mccr/qTiEDWDGE96/Qopva.jre Server: Microsoft-IIS/10.0 request-id: d3c10e4c-5e49-3a6f-0bca-0aa8eeb05a44 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: MWHPR13CA0010 X-RequestId: dd82cfc2-7512-45b0-82e8-afbaf83fa8be MS-CV: TA7B00lebzoLygqo7rBaRA.0 X-Powered-By: ASP.NET X-FEServer: MWHPR13CA0010 Date: Mon, 11 Oct 2021 22:38:46 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49807	52.97.183.162	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:46 UTC	3	OUT	GET /signup/liopolo/D7_2FrbWNPWoNOhc8CKrYUD/YRyHNJx0fY/hev8f_2BW8cdb94NA/BoQXWWXay0D_/2BZ8 Igd1CtC/8Zrwrke0SVrRun/EK5gc9OXOLgsoPgBxCQd1/LxUG0ef0GKyYljGP/_2FJyXjT77_2FZy/ZTRUMkvuvl3K PO1sTr/Mf1qwqvM6/BRuq80kiRu4imCu3Mccr/qTiEDWDGE96/Qopva.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: www.outlook.com
2021-10-11 22:38:46 UTC	4	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/signup/liopolo/D7_2FrbWNPWoNOhc8CKrYUD/YRyHNJx0fY/hev8f_2BW8 cdb94NA/BoQXWWXay0D_/2BZ8Igd1CtC/8Zrwrke0SVrRun/EK5gc9OXOLgsoPgBxCQd1/LxUG0ef0GKyYljGP/_2F JyXjT77_2FZy/ZTRUMkvuvl3KPO1sTr/Mf1qwqvM6/BRuq80kiRu4imCu3Mccr/qTiEDWDGE96/Qopva.jre Server: Microsoft-IIS/10.0 request-id: 4827db24-f7db-9519-6b3d-e535d1121fb8 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AM7PR03CA0018 X-RequestId: f1bbbeb9-c424-4847-91c0-206d8d6abcc1 MS-CV: JNsnSNv3GZVrPeU10RIfuA.0 X-Powered-By: ASP.NET X-FEServer: AM7PR03CA0018 Date: Mon, 11 Oct 2021 22:38:46 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49808	52.97.218.82	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:46 UTC	4	OUT	GET /signup/liopolo/D7_2FrbWNPWoNOhc8CKrYUD/YRyHNJx0fY/hev8f_2BW8cdb94NA/BoQXWWXay0D_/2BZ8 Igd1CtC/8Zrwrke0SVrRun/EK5gc9OXOLgsoPgBxCQd1/LxUG0ef0GKyYljGP/_2FJyXjT77_2FZy/ZTRUMkvuvl3K PO1sTr/Mf1qwqvM6/BRuq80kiRu4imCu3Mccr/qTiEDWDGE96/Qopva.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.office365.com

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:46 UTC	5	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: fee0e76a-0690-24c5-d39f-a0f3ac107e50 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: VI1PR0102CU003.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: VI1PR0102CA0087.EURPRD01.PROD.EXCHANGELABS.COM X-CalculatedBETarget: VI1PR04MB4495.eurprd04.prod.outlook.com X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: aufg/pAGxSTTn6DzrBB+UA.1.1 X-FEServer: VI1PR0102CA0087 X-Powered-By: ASP.NET X-FEServer: AS8PR04CA0081 Date: Mon, 11 Oct 2021 22:38:46 GMT Connection: close
2021-10-11 22:38:46 UTC	5	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49809	40.97.153.146	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:53 UTC	7	OUT	GET /signup/liopolo/rNcthdwaMuA/zHzDKpXzKq0_2F/hgSdOtaWvkDNGgYpqBLqh/fnirw5AL03xUm4gv/1SKD whrC85cQhDG/iqhTJ3hi9wsaeKx0vI/xO4E5YLZP/YP9uSugvYABSkowPk9S_/2B24KB1lGZ7pVE71wAB/PNLOy1DT AkJRmo3faOVpWQ/D9BP51I5FAmCi/mjxkDJSf_2B0/dO3cuvbU.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.com
2021-10-11 22:38:53 UTC	7	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/signup/liopolo/rNcthdwaMuA/zHzDKpXzKq0_2F/hgSdOtaWvkDNGgYpqBLqh/fn irw5AL03xUm4gv/1SKDwhrC85cQhDG/iqhTJ3hi9wsaeKx0vI/xO4E5YLZP/YP9uSugvYABSkowPk9S_/2B24KB1lG Z7pVE71wAB/PNLOy1DTAkJRmo3faOVpWQ/D9BP51I5FAmCi/mjxkDJSf_2B0/dO3cuvbU.jre Server: Microsoft-IIS/10.0 request-id: 556c818d-51ec-ad8d-c23c-618ef38fd56c Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: BN6PR2001CA0003 X-RequestId: d6343e44-52af-49e0-aabf-9bf1bd538048 MS-CV: jYFsVexRja3CPGGO84/VbA.0 X-Powered-By: ASP.NET X-FEServer: BN6PR2001CA0003 Date: Mon, 11 Oct 2021 22:38:52 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49810	52.97.218.66	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:53 UTC	8	OUT	GET /signup/liopolo/rNcthdwaMuA/zHzDKpXzKq0_2F/hgSdOtaWvkDNGgYpqBLqh/fnirw5AL03xUm4gv/1SKD whrC85cQhDG/iqhTJ3hi9wsaeKx0vI/xO4E5YLZP/YP9uSugvYABSkowPk9S_/2B24KB1lGZ7pVE71wAB/PNLOy1DT AkJRmo3faOVpWQ/D9BP51I5FAmCi/mjxkDJSf_2B0/dO3cuvbU.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: www.outlook.com

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:53 UTC	8	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/signup/liopolo/rNcthdwaMuA/zHzDKpXzKq0_2F/hgSdOtaWvkDNGgYpqB Lqh/fnirw5AL03xUm4gv/1SKDwhrC85cQhDG/iqhTJ3hi9wsaeKx0vI/xO4E5YLZP/YP9uSugvYABSkowPk9S_/2B2 4KB1lGZ7pVE71wAB/PNLOy1DTAkJRmo3faOVpWQ/D9BP51I5FAmCi/mjxkDJSf_2B0/dO3cuvbU.jre Server: Microsoft-IIS/10.0 request-id: fa41d79f-b084-e275-06fd-7c804baa2baf Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AS8PR04CA0017 X-RequestId: 5790813c-b01e-46a4-ac89-6c67c15fc018 MS-CV: n9dB+oSwdeIG/XyAS6orrw.0 X-Powered-By: ASP.NET X-FEServer: AS8PR04CA0017 Date: Mon, 11 Oct 2021 22:38:52 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49811	52.97.137.210	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:38:53 UTC	9	OUT	GET /signup/liopolo/rNcthdwaMuA/zHzDKpXzKq0_2F/hgSdOtaWvkDNGgYpqBLqh/fnirw5AL03xUm4gv/1SKD whrC85cQhDG/iqhTJ3hi9wsaeKx0vI/xO4E5YLZP/YP9uSugvYABSkowPk9S_/2B24KB1lGZ7pVE71wAB/PNLOy1DT AkJRmo3faOVpWQ/D9BP51I5FAmCi/mjxkDJSf_2B0/dO3cuvbU.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: outlook.office365.com
2021-10-11 22:38:53 UTC	9	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: 463ae588-6705-a5a4-dc70-c20dde540b89 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: HE1PR0202CU001.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: HE1PR0202CA0016.EURPRD02.PROD.OUTLOOK.COM X-CalculatedBETarget: HE1P194MB0201.EURP194.PROD.OUTLOOK.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: iOU6RgVnpKXccMIN3lQLiQ.1.1 X-FEServer: HE1PR0202CA0016 X-Powered-By: ASP.NET X-FEServer: AM6P194CA0062 Date: Mon, 11 Oct 2021 22:38:53 GMT Connection: close
2021-10-11 22:38:53 UTC	10	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49827	13.82.28.61	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:39:27 UTC	11	OUT	GET /mail/liopolo/5hHdOh6aVGIiN/xm3v7_2B/EkShunhzAo7MsZ9CmkqFWtX/3z_2Bns4ON/91CWMsZkh9K0L_ 2FK/DGWBtSEwajEJ/0TtpREbudd5/QgJK102N2T9j48/a7_2B8h2NmEQ_2FO6HINr/eS5x2dWmrnxEuUas/E6VYZyo ESNredc4/JUFmKkMiSye_2BBKeH/JexZCfmhU/vSKjW_2B8KOY/RYzBQt1.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: msn.com

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:39:27 UTC	12	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.msn.com/mail/liopolo/5hHdOh6aVGIiN/xm3v7_2B/EkShunhzAo7MsZ9CmkqFWtX/3z_2Bns4ON/91CWMsZkh9K0L_2FK/DGWBtSEwajEJ/0TtpREbudd5/QgJK102N2T9j48/a7_2B8h2NmEQ_2FO6HINr/eS5x2dWmrnxEuUas/E6VYZyoESNredc4/JUFmKkMiSye_2BBKeH/JexZCfmhU/vSKjW_2B8KOY/RYzBQt1.jre Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Date: Mon, 11 Oct 2021 22:39:26 GMT Connection: close Content-Length: 380
2021-10-11 22:39:27 UTC	12	IN	Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 73 6e 2e 63 6f 6d 2f 6d 61 69 6c 2f 6c 69 6f 70 6f 6c 6f 2f 35 68 48 64 4f 68 36 61 56 47 49 69 4e 2f 78 6d 33 76 37 5f 32 42 2f 45 6b 53 68 75 6e 68 7a 41 6f 37 4d 73 5a 39 43 6d 6b 71 46 57 74 58 2f 33 7a 5f 32 42 6e 73 34 4f 4e 2f 39 31 43 57 4d 73 5a 6b 68 39 4b 30 4c 5f 32 46 4b 2f 44 47 57 42 74 53 45 77 61 6a 45 4a 2f 30 54 74 70 52 45 62 75 64 64 35 2f 51 67 4a 4b 31 30 32 4e 32 54 39 6a 34 38 2f Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.msn.com/mail/liopolo/5hHdOh6aVGIiN/xm3v7_2B/EkShunhzAo7MsZ9CmkqFWtX/3z_2Bns4ON/91CWMsZkh9K0L_2FK/DGWBtSEwajEJ/0TtpREbudd5/QgJK102N2T9j48/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49829	13.82.28.61	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 22:39:34 UTC	12	OUT	GET /mail/liopolo/QoeEw7znNY9KuZLPv/PhlDvAFg0Bnn/nVx6DnTynJS/Jqe2AOjRD8vYJs/PuqBLIn3Zd37OXyJlwD7Q/FiLhjKnVW_2ByswX/LXphFosRYtREZOL/Q6wDOp8ES889SSlI1S/AFbHRrWLn/_2F7R_2FVhgDELEonTCy/KSLPzpnW0YF_2FoB4Xy/kHR_2F88KI6KqxU9hJvbKE/it_2FLM35/c.jre HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: msn.com
2021-10-11 22:39:34 UTC	13	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.msn.com/mail/liopolo/QoeEw7znNY9KuZLPv/PhlDvAFg0Bnn/nVx6DnTynJS/Jqe2AOjRD8vYJs/PuqBLIn3Zd37OXyJlwD7Q/FiLhjKnVW_2ByswX/LXphFosRYtREZOL/Q6wDOp8ES889SSlI1S/AFbHRrWLn/_2F7R_2FVhgDELEonTCy/KSLPzpnW0YF_2FoB4Xy/kHR_2F88KI6KqxU9hJvbKE/it_2FLM35/c.jre Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Date: Mon, 11 Oct 2021 22:39:33 GMT Connection: close Content-Length: 377
2021-10-11 22:39:34 UTC	13	IN	Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 73 6e 2e 63 6f 6d 2f 6d 61 69 6c 2f 6c 69 6f 70 6f 6c 6f 2f 51 6f 65 45 77 37 7a 6e 4e 59 39 4b 75 5a 4c 50 76 2f 50 68 6c 44 76 41 46 67 30 42 6e 6e 2f 6e 56 78 36 44 6e 54 79 6e 4a 53 2f 4a 71 65 32 41 4f 6a 52 44 38 76 59 4a 73 2f 50 75 71 42 4c 49 6e 33 5a 64 33 37 4f 58 79 4a 6c 77 44 37 51 2f 46 69 4c 68 6a 4b 6e 56 57 5f 32 42 79 73 77 58 2f 4c 58 70 68 46 6f 73 52 59 74 52 45 5a 4f 4c 2f 51 36 77 Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.msn.com/mail/liopolo/QoeEw7znNY9KuZLPv/PhlDvAFg0Bnn/nVx6DnTynJS/Jqe2AOjRD8vYJs/PuqBLIn3Zd37OXyJlwD7Q/FiLhjKnVW_2ByswX/LXphFosRYtREZOL/Q6w

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 7036 Parent PID: 5284

General

Start time:	00:36:03
Start date:	12/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\616412739e268.dll'
Imagebase:	0xd40000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.916793229.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.916426520.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.916847995.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.916379765.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.1049081119.000000000383F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.916579363.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.960454814.0000000003A3B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.917263832.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.1185910848.00000000037C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.916716758.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.859623257.0000000001390000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.916652805.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.1006058312.000000000393D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.916501324.0000000003BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.1185750269.0000000003559000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 7040 Parent PID: 7036

General

Start time:	00:36:04
Start date:	12/10/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\616412739e268.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7072 Parent PID: 7036

General

Start time:	00:36:04
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\616412739e268.dll,BeGrass
Imagebase:	0x910000
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_1, Description: Yara detected Ursnif, Source: 00000002.00000003.815784536.0000000003220000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7052 Parent PID: 7040

General

Start time:	00:36:04
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\616412739e268.dll',#1
Imagebase:	0x910000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.974874720.000000000573B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.1187092392.00000000054C0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.930983342.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.930624015.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.1020193164.000000000563D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.930910657.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.931064048.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.817641494.0000000003420000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.930863354.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.1063376109.000000000553F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.931519942.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.931136929.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.930715901.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.1186977706.0000000005229000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.930775995.00000000058B8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 1364 Parent PID: 7036

General

Start time:	00:36:09
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\616412739e268.dll,Fieldeight
Imagebase:	0x910000
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_1, Description: Yara detected Ursnif, Source: 00000004.00000003.843034391.00000000008A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6464 Parent PID: 7036

General

Start time:	00:36:17
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\616412739e268.dll,Often
Imagebase:	0x910000
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_1, Description: Yara detected Ursnif, Source: 00000005.00000003.855981301.0000000002EC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000003.888775678.0000000004D09000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 6452 Parent PID: 7072

General

Start time:	00:37:46
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7072 -s 636
Imagebase:	0x10e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 6824 Parent PID: 1364

General

Start time:	00:37:51
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1364 -s 644
Imagebase:	0x10e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Analysis Process: WerFault.exe PID: 6368 Parent PID: 6464

General

Start time:	00:37:56
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6464 -s 632
Imagebase:	0x10e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Disassembly

Code Analysis