ID: 500299
Sample Name: B6VQd36tt6.dll
Cookbook: default.jbs
Time: 22:19:56
Date: 11/10/2021
Version: 33.0.0 White Diamond

Table of Contents

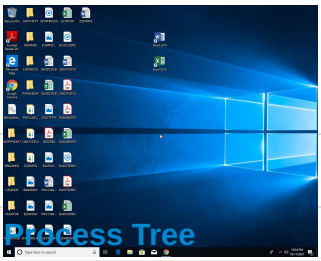
Windows Analysis Report B6VQd36tt6.dll

Overview

General Information

Sample Name:	B6VQd36tt6.dll
Analysis ID:	500299
MD5:	c4c060ec6b1e42…
SHA1:	3ef84847fceb31b..
SHA256:	47715e42539828..
Tags:	BRT dll geo Gozi ISFB ITA Ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

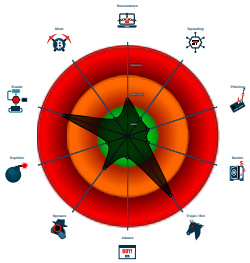
Ursnif

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



- **System is w10x64**
- loaddll32.exe (PID: 6116 cmdline: loaddll32.exe 'C:\Users\user\Desktop\B6VQd36tt6.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4024 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\B6VQd36tt6.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4720 cmdline: rundll32.exe 'C:\Users\user\Desktop\B6VQd36tt6.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4892 cmdline: rundll32.exe C:\Users\user\Desktop\B6VQd36tt6.dll,BeGrass MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4364 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 864 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5780 cmdline: rundll32.exe C:\Users\user\Desktop\B6VQd36tt6.dll,Fieldeight MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2836 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5780 -s 840 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 724 cmdline: rundll32.exe C:\Users\user\Desktop\B6VQd36tt6.dll,Often MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4736 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 724 -s 636 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"UmEkthy8LQToWYBqtBaWyLn/P1d2KjpXi9nl2is1X7NEi7AW4Al92U7HvBiCwWHgXhs6UyTZ7q6npv3YCi+rPS7xAyorWWgcyyviEpE9CETDXviZ72XZkxmen4ztvEtct+obFAEe0tiXOsfOcC8xDsI0CHPpvmUknsexTYqAJgwcghgx
1mGHx/yFM4fnPYw4mFFE6bVI7eMnbu1CuunRmAVRDHZ7MAS7zSkAmYjeo1zAzRnOEWgblRHwenmwlBtp0SFGuYCGVe3TZZ4Nndgpd5xpSeLOoSZi/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
00000003.00000003.499708236.00000000057E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000002.785119761.00000000053F0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.638534724.0000000002D1F000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.498145572.00000000057E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.506367708.0000000003098000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.50394a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.6e610000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.a6a31a.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.loaddll32.exe.85a31a.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.3.rundll32.exe.d7a31a.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 13 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

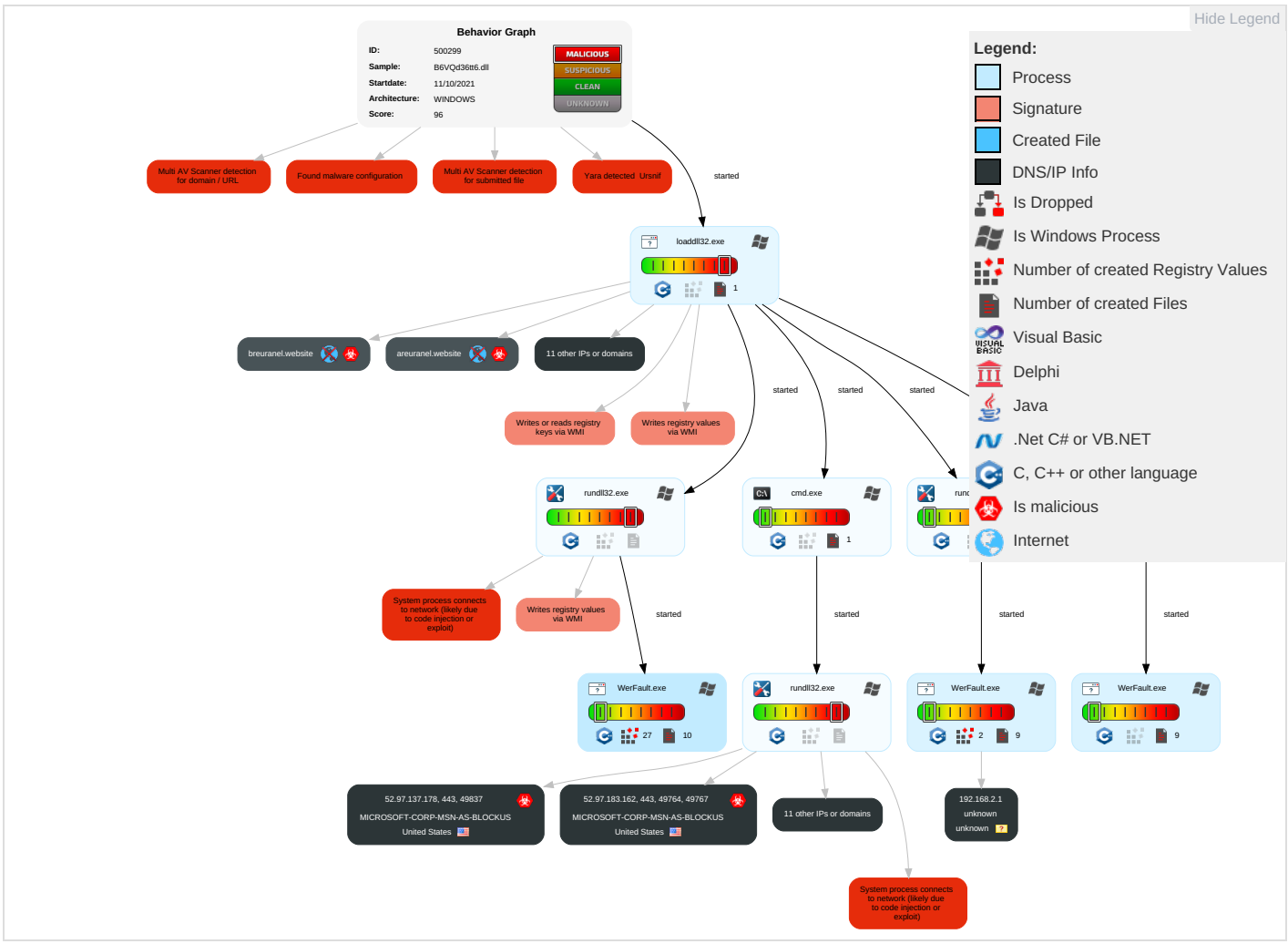
Remote Access Functionality:

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	Networ Effects
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 1 2	Masquerading 1	Input Capture 1	System Time Discovery 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesc Insecu Networ Commu
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

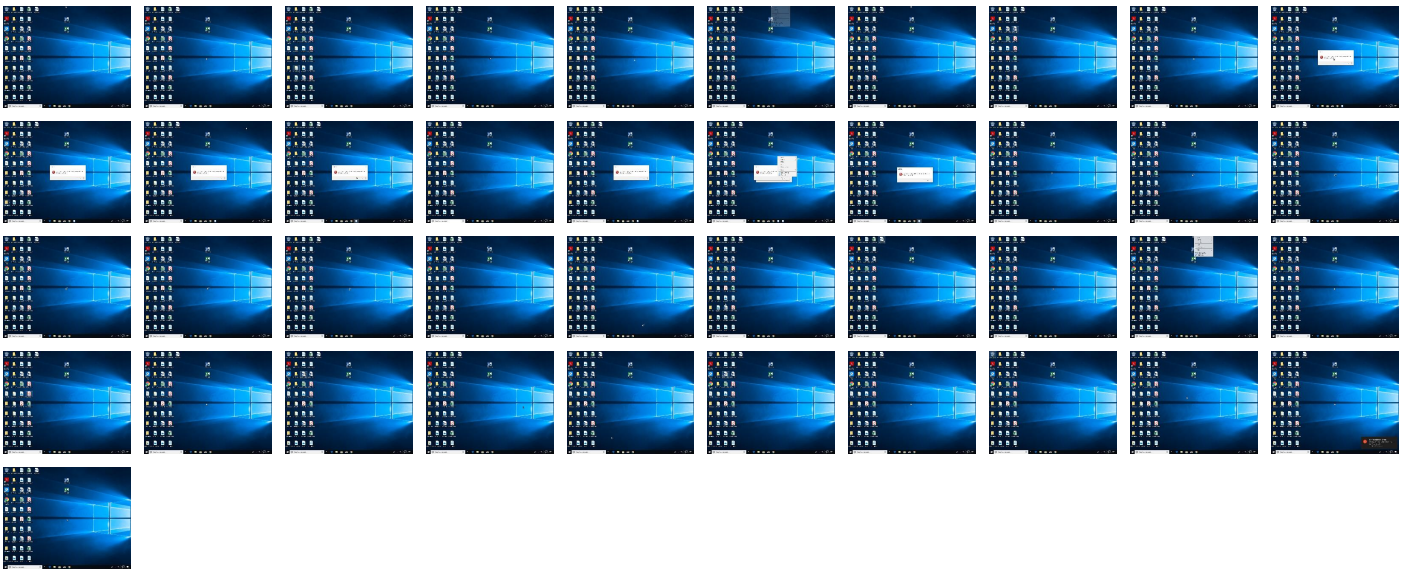
Behavior Graph



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
B6VQd36tt6.dll	17%	Virustotal		Browse
B6VQd36tt6.dll	24%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.830000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.3050000.0.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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
msn.com	13.82.28.61	true	false		high
outlook.com	40.97.164.146	true	false		high
HHN-efz.ms-acdc.office.com	40.101.91.82	true	false		high
FRA-efz.ms-acdc.office.com	52.97.151.18	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://msn.com/mail/liopolo/A1Qp_2BWzai2O5/xac_2BRG3wzSiIIBjQnWR/yH8MK_2FDeyVZ7zs/MmgvT5kbS5J14SI/50tiJJe1m8aJQ2XT7T/rIRQt7iCb/CwoKyLq7nfSWQHvgpN7o/BCyQHF5XZOebIuFzT_2/BFFOtw4QHhKTLswkkvF9vD/aY9DT6JVICQxS/piqcZUHz/pQlXCrwUL0BTmEd_2FLWL2L/RH2uj8PySJ/d2LKLIyBddk3_2FhT/H.jre	false		high
http://https://outlook.com/signup/liopolo/7RiyOegViATthNX4pt/E65VkdFK0/peIG_2BaG1SxNKYOcdXs/80APf88JeQpK_2BfrxB/1_2B2_2FNDAEnuSdYMUmdr/BpxBwvlUzTu3W/v3tDiaIH/uhnULhLXCDfDONp_2FCc03F/ZkPsDATWsR/KNPTfNdkqqbWMwLBy/xU_2Bk46LKIT/9_2FOKzik9g/v8mZTndKcyg89a/ELxzR_2BALqku0rQMRn2U/KVAF7ruVq/mnKq.jre	false		high
http://https://outlook.com/signup/liopolo/f5kvQFsIv4wED/j69h8mSZ/xzzTxsSNNb1pIF2nd0zyLKL/oW0UsUUi2h/1n_2FrPb8KlH0Zm6I/DMN_2B2Rb3dP/VgvW0BFn0fE/SZJzWGdiy3m5qM/ymewVR1TpC9Ou3wlV9Okm/omWH_2FxfhHZzw96/HP0eihm9FW1uN9V/ykWA9NBBnDVcWXTKfE/JwgC0Jx4CafbQ/qgLsjM_2/F.jre	false		high
http://https://www.outlook.com/signup/liopolo/7RiyOegViATthNX4pt/E65VkdFK0/peIG_2BaG1SxNKYOcdXs/80APf88JeQpK_2BfrxB/1_2B2_2FNDAEnuSdYMUmdr/BpxBwvlUzTu3W/v3tDiaIH/uhnULhLXCDfDONp_2FCc03F/ZkPsDATWsR/KNPTfNdkqqbWMwLBy/xU_2Bk46LKIT/9_2FOKzik9g/v8mZTndKcyg89a/ELxzR_2BALqku0rQMRn2U/KVAF7ruVq/mnKq.jre	false		high
http://https://msn.com/mail/liopolo/XqCHqVDXW8CZUpeu5peN_2/FydjgYTJtTmoC/fAo34oef/chWHLvpFFUOYdiWXbNbnYW0/Rfy3HU21P_/2FwjKpEqeFo_2FxU6/0A_2BR4J2MVl/hx12NRqsjmC/kkNl1wduKuFf8Q/FUG3Ocqqzs1x_2BibuPx6/9auuC1P5josci_2B/vyxmzUWJ7gSzOqo/Jt7rxzWzdI7AYIGNrQ/e7oR22vyh/Me9W1V8u/5SwAx9Su/B.jre	false		high
http://https://outlook.com/signup/liopolo/5R03kGEb4YkHyvd/vrgMCXbUCWgL9mS74E/ZNV_2FT7r/A0OAE579SB7Hx3A4JeNe/QST70In3HBC_2F_2Flg/hEE1oqV04Tcb_2BXZ4DwC_/2BDjxaFgiu1Kq/cZhA7baN/ystZ_2FV5yPDIe8qQfN_2Fy/gQ02q5YT1n/eawFPHFBcfhAYskcF/Z0kyVxsdmmeN/mzjXdayEo/OIVTn_2Fwlw/Fu.jre	false		high
http://https://www.outlook.com/signup/liopolo/f5kvQFsIv4wED/j69h8mSZ/xzzTxsSNNb1pIF2nd0zyLKL/oW0UsUUi2h/1n_2FrPb8KlH0Zm6I/DMN_2B2Rb3dP/VgvW0BFn0fE/SZJzWGdiy3m5qM/ymewVR1TpC9Ou3wlV9Okm/omWH_2FxfhHZzw96/HP0eihm9FW1uN9V/ykWA9NBBnDVcWXTKfE/JwgC0Jx4CafbQ/qgLsjM_2/F.jre	false		high
http://https://outlook.office365.com/signup/liopolo/5R03kGEb4YkHyvd/vrgMCXbUCWgL9mS74E/ZNV_2FT7r/A0OAE579SB7Hx3A4JeNe/QST70In3HBC_2F_2Flg/hEE1oqV04Tcb_2BXZ4DwC_/2BDjxaFgiu1Kq/cZhA7baN/ystZ_2FV5yPDIe8qQfN_2Fy/gQ02q5YT1n/eawFPHFBcfhAYskcF/Z0kyVxsdmmeN/mzjXdayEo/OIVTn_2Fwlw/Fu.jre	false		high
http://https://www.outlook.com/signup/liopolo/5R03kGEb4YkHyvd/vrgMCXbUCWgL9mS74E/ZNV_2FT7r/A0OAE579SB7Hx3A4JeNe/QST70In3HBC_2F_2Flg/hEE1oqV04Tcb_2BXZ4DwC_/2BDjxaFgiu1Kq/cZhA7baN/ystZ_2FV5yPDIe8qQfN_2Fy/gQ02q5YT1n/eawFPHFBcfhAYskcF/Z0kyVxsdmmeN/mzjXdayEo/OIVTn_2Fwlw/Fu.jre	false		high
http://https://outlook.office365.com/signup/liopolo/f5kvQFsIv4wED/j69h8mSZ/xzzTxsSNNb1pIF2nd0zyLKL/oW0UsUUi2h/1n_2FrPb8KlH0Zm6I/DMN_2B2Rb3dP/VgvW0BFn0fE/SZJzWGdiy3m5qM/ymewVR1TpC9Ou3wlV9Okm/omWH_2FxfhHZzw96/HP0eihm9FW1uN9V/ykWA9NBBnDVcWXTKfE/JwgC0Jx4CafbQ/qgLsjM_2/F.jre	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://msn.com/mail/liopolo/yn_2BPYQmJ20vgPRL3/3wjWE1bwH/DDPf_2FmyfN4qjiroAKh/7sxv413IrGA7KcA9Hu0/BYfxtbSdLKzFinzGkJGdmk/P_2Fifx7koRFQ/MIG6rk6P/jRWWDjWjz87k5xmFJxsJqsu/JDVOEV0_2F/rb6v_2FY3MQLb6_2F/gkDS2luFhYah/H5Mm0Y9iZUr/9_2FNXlrb5xId9/cAon_2FllX9wfUzSs9jRy/iECEQNsAU7oK/0.jre	false		high
http://https://outlook.office365.com/signup/liopolo/7RiyOegViATthNX4pt/E65VkdFK0/peIG_2BaG1SxNKYOcdXs/80APf88JeQpK_2BfrxB/1_2B2_2FNDAEnuSdYMUmdr/BpxBwvlUzTu3W/v3tDialH/uhnULhLXCDfDONp_2FCc03F/ZkPsDATWsR/KNPTfNdkqqbWMwLBy/xU_2Bk46LKIT/9_2FOKzik9g/v8mZTndKcyg89a/ELxzR_2BALqku0rQMRn2U/KVAF7ruVq/mnKq.jre	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
40.97.164.146	outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.101.60.2	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.101.91.82	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.151.114	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.151.18	FRA-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.82.28.61	msn.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.137.178	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
52.97.183.162	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	500299
Start date:	11.10.2021
Start time:	22:19:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	B6VQd36tt6.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:	39
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@26/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7% (good quality ratio 6.6%) • Quality average: 79.9% • Quality standard deviation: 28.6%
HCA Information:	Failed
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
22:22:40	API Interceptor	8x Sleep call for process: loaddll32.exe modified
22:22:53	API Interceptor	7x Sleep call for process: rundll32.exe modified
22:22:58	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
40.97.164.146	611242387c2b3.dll	Get hash	malicious	Browse	
	611237846402f.dll	Get hash	malicious	Browse	
	FuiZSHt8Hx.dll	Get hash	malicious	Browse	
	http://https://live-microsoft.app.link/81e6d30/verify/recovery	Get hash	malicious	Browse	
	78lette.exe	Get hash	malicious	Browse	
	12file.htm .exe	Get hash	malicious	Browse	
	3HnStrg8u06.exe	Get hash	malicious	Browse	
	57C5fDSKCrJU.exe	Get hash	malicious	Browse	
	7transcrip.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
40.101.60.2	32noemai.exe	Get hash	malicious	Browse	
	62lette.exe	Get hash	malicious	Browse	
	FINANCE_D0C-989261.pdf	Get hash	malicious	Browse	
40.101.91.82	PROFORMA INVOICE -PI6120..html	Get hash	malicious	Browse	
	http://x.co/6ngvm	Get hash	malicious	Browse	
	http://https://www.rheat.xyz/$xi-in/index.php?!ch!m@9!	Get hash	malicious	Browse	

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	nFkQ33d7Ec.exe	Get hash	malicious	Browse	• 104.47.53.36
	QE66HWdeTM.exe	Get hash	malicious	Browse	• 40.93.207.0
	2H69p1kjC4.exe	Get hash	malicious	Browse	• 40.93.207.1
	SEYpTxOaaR.exe	Get hash	malicious	Browse	• 104.47.53.36
	fxXx5zeMoZ.exe	Get hash	malicious	Browse	• 104.47.53.36
	CcXHF1vwBV.exe	Get hash	malicious	Browse	• 40.93.207.1

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MICROSOFT-CORP-MSN-AS-BLOCKUS	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
	in7BcpKNoa.exe	Get hash	malicious	Browse	• 40.93.212.0
	xiaomi-home.apk	Get hash	malicious	Browse	• 104.45.180.93
	canon-camera-connect.apk	Get hash	malicious	Browse	• 104.45.180.93
	aXNdDIO708.exe	Get hash	malicious	Browse	• 104.47.53.36
	uT9rwkGATJ.dll	Get hash	malicious	Browse	• 52.98.208.114
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 20.189.173.20

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	aVFOmbW2t7.dll	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	gxJ83rJkgw.msi	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	yR4AxlwcWJ.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BsyK7FB5DQ.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	SGfGZT66wD.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	uT9rwkGATJ.dll	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	XK1PLPuwjL.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	pHEiqE9toa.msi	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	SecuriteInfo.com.W32.AIDetect.malware2.24481.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	vH0SHswvrb.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	NM0NyvZi8O.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	yOTzv1Qz0n.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	SWaTAV7EdD.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SKMC07102021.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	50r72lVfM0.msi	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	83ONlZMwS9.msi	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	Dxr7myLbG2.msi	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162
	tributaria.exe	Get hash	malicious	Browse	• 40.97.164.146 • 40.101.60.2 • 40.101.91.82 • 52.97.151.18 • 13.82.28.61 • 52.97.151.114 • 52.97.137.178 • 52.97.183.162

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_b6db214dd89db871c3cf2d8284ebed8c4377271_82810a17_0a11246a\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12042
Entropy (8bit):	3.765339362044577
Encrypted:	false
SSDEEP:	192:UF+6ie0oXnHBUZMX4jed+5/u7saS274lt7ce:16ioXHBUZMX4jeU/u7saX4lt7ce
MD5:	277FFDA2256ED46D46653F6DD3E3FC2B
SHA1:	460F928A7D5DF2C6185271B78E0BAFCFA83CFBF7
SHA-256:	10E6BD9A1E7946EF8E95295B568F1EA61DBC958936719D387BD2F3B7E9124C67
SHA-512:	6C2B295979991CC3B27C0A9FB0F2B1C21B5AEBF93C5B5A70BDF5EF3CCE8CBFC44005E63D079A30E54B1649E17C2216490A65D8D71F02BBD06B18A02CE4980D50
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_b6db214dd89db871c3cf2d8284ebed8c4377271_82810a17_0a11246a\Report.wer	
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.=.1.3.2.7.8.4.8.9.7.7.1.8.0.7.9.2.4.5.....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.=.1.3.2.7.8.4.8.9.7.8.5.3.0.7.8.7.8.0.....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.3.0.7.d.7.4.-.0.d.6.2.-.4.1.7.b.-.9.1.e.7.-.d.f.c.3.1.2.a.3.4.3.7.4.....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.=.2.1.8.9.4.e.1.0.-.5.c.1.9.-.4.b.0.0.-.8.2.8.1.-.f.7.f.b.f.f.4.8.f.a.c.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.=.0.0.0.0.1.6.9.4.-.0.0.0.1.-.0.0.1.7.-.6.b.8.3.-.b.b.f.1.2.8.b.f.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_b6db214dd89db871c3cf2d8284ebed8c4377271_82810a17_100904dc\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12046
Entropy (8bit):	3.76447609928904
Encrypted:	false
SSDEEP:	192:Ad+cXiD90oXsHBUZMX4jed+x/u7saS274It7cT:fMivX0BUZMX4je8/u7saX4It7cT
MD5:	6966D2DE44EA08463E24DC6266A2BD41
SHA1:	911E751B87C1897695187DE7908162AD7D038969
SHA-256:	D9BDFF4D0A3F508176975EFAFDF05D2B054631B19B3F2A50ACD16C778C079452
SHA-512:	A454046986DFFF654AF9190CB5F78F6140CA0D56EFED5899412D51031B1B8C3B7D58DEE465F42CDBEDED5ACBBF3B3AF81476CA9812EB583324EEADD1BF416EC5
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.=.1.3.2.7.8.4.8.9.7.7.6.9.9.1.1.8.6.4.....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.=.f.f.a.a.4.c.e.d.-.e.d.2.4.-.4.4.a.d.-.9.c.7.0.-.2.6.9.f.7.b.8.d.f.6.f.e.....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.=.0.0.0.0.1.3.1.c.-.0.0.0.1.-.0.0.1.7.-.f.2.5.4.-.c.0.e.f.2.8.b.f.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_b6db214dd89db871c3cf2d8284ebed8c4377271_82810a17_138537a4\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):	3.765226129606169
Encrypted:	false
SSDEEP:	192:p5PiC0oXLHBUZMX4jed+5/u7saS274It7ch:3PiEXrBUZMX4jeU/u7saX4It7ch
MD5:	0F87890F31929D46E5A324BE411D2771
SHA1:	F4D138ED901D0135ED6BB5E44388B7B98049B4FE
SHA-256:	396C82499FDCB028697834E0C62EC26902DE680353A1026F52440EAE35B596F6
SHA-512:	BD659BA4494ECDFF31420ACCDE586D5368017F55142FFBC306D02E8D8BD83FABA4B2F17B7021B225F746CFB493A1891E6DABF83EFE96071598CBA0EED440D4CE
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.=.1.3.2.7.8.4.8.9.7.7.8.4.1.4.6.9.4.9.....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.=.1.3.2.7.8.4.8.9.7.9.0.2.2.7.1.1.2.2.....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.=.2.9.2.5.f.3.0.0.-.c.3.5.b.-.4.8.f.9.-.b.3.8.e.-.f.7.1.8.6.1.e.9.d.2.4.c.....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.=.5.c.b.e.1.b.6.7.-.4.2.5.4.-.4.9.8.8.-.b.3.5.9.-.8.9.4.e.9.4.c.3.5.d.0.e.....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.=.0.0.0.0.0.2.d.4.-.0.0.0.1.-.0.0.1.7.-.b.5.1.8.-.d.e.f.5.2.8.b.f.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\WER5812.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Oct 12 05:22:46 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	34688
Entropy (8bit):	2.4160053350772017
Encrypted:	false
SSDEEP:	192:2tw6oTiQYP5MFmpISGG+0oszTU70dIQlI+qSnUHvt:Cl0iQmqFo/+0oszTHlICUHF
MD5:	69E0098DB631036EA0E7709B73A4F1E9
SHA1:	DF2D3146532E75A09BC35F01EC76D0B5FCDC82EB
SHA-256:	73F8F7567A24A1BEAC9B127BC8C45CEE542B9C69DBD7778B1203B3AD9FDF8CD6
SHA-512:	7E9DB7BCD6B553237108465F1B1BEF6F7ADD51973855857D98C1A108F460E08E41EAED621FACB460ACDC5832DC004E7EAA3DC88DA1D12B6A49C835037FE6F814
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5812.tmp.dmp	
Preview:	MDMP..... .....ea.....U.....B.....GenuineIntelW.....T.....9.ea!.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FB4.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):	8410
Entropy (8bit):	3.694304201114169
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiKjN6qYXt6YiG6njLxpmOfgmf8KSjCprk89bWrsfRpym:RrlsNisN69t6Yz6XxpmOfgmf8KSqWwf7
MD5:	EFB89DDE8AB49502174519293907AF20
SHA1:	04E6F1303221AC02094CF8518300D818472DD6FC
SHA-256:	8D2E010E54013D580C46E65ECCA4AEB8C476C3ABE0ACE86EAD794786DF94FEC2
SHA-512:	0EACD5C1C8962283DE088655A9287934F52F2BCCA7350850F57E6A7BDBEA7DE4CA54BF968C8E773096F8C25FBECC4AA5870701575415BC09B8CE6E0B4CD37F EE
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.>.4.8.9.2.<./.P.i d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER64C6.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):	4.4824130026256634
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUrJgtWI9zuC3ugWSC8Bo8fm8M4JCds0MFN+q8vjs0E4SrSNd:uITfA02SNPJSUKREDWNd
MD5:	57567DB7EFBD3698518DA782470DDB05
SHA1:	9F9EEF89CA1DF1F6C49BC541985BB8893E0FF193
SHA-256:	E72BEB87956ABF950B1AF529948E60BA4DB43E5BAED0F1A982CB3153F603E041
SHA-512:	32A2BDE59E8F5108F7D437EF56376DCDBB76AFD1BBFDDD8E759D2C8687D94765858EB58DEBC4E0A923FE1984AD642A9D152CF1F753EBE96B7585B7A5E480A D5
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="1206153" />.. <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\WER74B2.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Oct 12 05:22:57 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	35410
Entropy (8bit):	2.3895077902606845
Encrypted:	false
SSDEEP:	192:zNHKylVGslNP5MFmpISGG+0fsztU+PyVUFEQ60J0TQnHKhz1:BqlsnqFo/+0fsztBS0EQcsHKB1
MD5:	D9B9F9C0C0CE14A6C3960BDB2EFE1B8A
SHA1:	C3D13D526D858507F7731F290483DE6625468F1C
SHA-256:	32E412A27B4E5261B9048FF657B36A92543E7CA13711F21325C213E3F4DE3253
SHA-512:	C7FD68FC0008261FEA3AD726FFE4D5451F5AEF1D079B9D95DA4E15EC01F4E9DF6D62D9D3922FD55A64DFFBF2782F9874F8BD6123CEEA8036B386FC5CE28E17 A4
Malicious:	false
Preview:	MDMP..... .....ea.....U.....B.....GenuineIntelW.....T.....<.ea!.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CB0.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):	8410
Entropy (8bit):	3.6968806045802087
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/MA6d6Yiz6egmf8KSjCprI89b5bsfZlTm:RrlsNir6d6Y26egmf8KSu5gfu
MD5:	EBAAF589AB7642BA9E2C2FCA4BA7643F
SHA1:	8A163AEF211471C8A58515B29BA2CFEF3ABA6407
SHA-256:	2AF27F59684D80A42AFA5AB9C10B2F48EC5BBA45254883C77A765223025D295E
SHA-512:	28736FB6DC05101C36D253357D0952D6F39C738465BFFE56EBC1277A1B423D6CFBB3CF22C11FB990B44A119F924717B32870A77C13B98E955F99A5A17850EE9E
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.>.5.7.8.0.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E83.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Oct 12 05:23:02 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	34358
Entropy (8bit):	2.4529576435604046
Encrypted:	false
SSDEEP:	192:7YWQ8iDfq/EQU6MP5MFmpISGG+0ZsztUw5x1lCzQxn0u9nPOUro:UWQ8yZQU6KqFo/+0ZsztbnC8xTPhro
MD5:	CBC4BA1DD7DB92DCAA1B6FEE4F65D535
SHA1:	4633B03471C838D738A9230275E7D7CD46D114F1
SHA-256:	1EB278AC6DD52B65E6D854C38AD72479B120D420254880D01BAD6A4E0FFA9BD9
SHA-512:	02168ADB945C123FA25E324486FF0EE86B925685A725BD53C66435787E8A0A8A6115AC0D3D05DA759C93DE4D9133BAF3F709CB7A36761FE4C98DD0BE0BA9BD 2
Malicious:	false
Preview:	MDMP..... .....ea.....U.....B.....GenuineIntelW.....T.....C.ea!.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER90C7.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):	4.48394283736822
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUrJgtWI9zuC3ugWSC8BX8fm8M4JCds0MFlQk+q8vjs0X4SrSmd:uITfA02SNCJSGKRXDWmd
MD5:	FC7A4C4098B95440D6BF73B0D44641D5
SHA1:	5713B15627CBF4B44277F821286BF4BC9E10E966
SHA-256:	CBF9A06B7C5F3235E7F78416638F61EEC6FB7230FF9ED4CA6053B2BB1B133116
SHA-512:	4F1EB3DBCA84729454BB7D5B7B84523AEF03F39BF612078A68F292374A462710C06F5268597A6DD2CE63E0106844164315CE6D9B356F09269AD944CC79572477
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="1206153" />.. <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\WER9FBB.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):	8406
Entropy (8bit):	3.6964337125203657
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FBB.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNi8x6b6Yiy6egmf8KSjCprd89beJsf2Km:RrlsNiq6b6Y36egmf8KSheify
MD5:	C861E33E7AC2C616B1134851B9572611
SHA1:	87C3BDA6468AF3574B321E7C8FB67C4D2BB1EA1A
SHA-256:	1448514E2F079972558625A8BD6F8598B3726E3EFDD36D3DB7BEA7E3D48A236D
SHA-512:	E69CEE46F0A487E31148F53F13D8F5D0060AF255AEEE4AE52BAE42B0F8D5CD4197EE8B4343F95173075860012A20402387763D8876377BF65ADF143EEF9F72C8
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.>.7.2.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA5F5.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):	4.484146537656321
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUrJgtWI9zuC3ugWSC8BfK8fm8M4JCds0MFG/+q8vjs0X4SrSpd:uITfA02SNpJSFKRXDWpd
MD5:	38A92FED97B3B67E713096B18C5E2945
SHA1:	E804A79C99EB3D9002A7FEFC10C95107BC42B30A
SHA-256:	35A4309E917383635996A11E469EC2BDFD1603F4332E58B8F739B1EAD08331AD
SHA-512:	F45EA9B7B0D3C7D656210F0C49BC8ACE84ACABF62094E56B955171D7C14F85619A1FCF9794346536925928OC92EE70E7A6A56B791709F4CEB44B295790BEDE6
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="1206153" />.. <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 Windows
Entropy (8bit):	6.67002840473361
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:	B6VQd36tt6.dll
File size:	718336
MD5:	c4c060ec6b1e42d70972d0af66a04e66
SHA1:	3ef84847fceb31b8814c12c94c57c72a5281d6f5
SHA256:	47715e425398283d53019c270311ad0c709f660048d2f884d5116d80b983743f
SHA512:	5553d68867af378d347620208b35d4d6261526770cf2a47884f0eff17392cedfa91ab491265717a459b4ccbe43f490a90caaf9289b9f92e8cd63140710e9ca78
SSDEEP:	12288:QUAQSxT6fDEr8Np6b/rPPsjosrS9aEoe+0JCym+4YJAOSVUNcuHIGF4uW/XPGAsx:Qz3xT6fq8Np6bTPPaBreaZlYCOSVolam
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..Ox.`.x.`.x.`..~..{.`.q...m.`...b.|.`...e.q.`...c.l.`..~..o.`.x.a...`...e...`...`.y.`...`.y.`.x...y.`...b.y.`.Richx.`.....

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:	0x5F6FEFFF [Sun Sep 27 01:50:55 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:	8acc1c3be9064cb55c8e3d7147f3d7c3

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	6.75461975802	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7b000	0x2e586	0x2e600	False	0.556377400606	data	5.60164615331	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

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 11, 2021 22:22:51.374481916 CEST	192.168.2.7	8.8.8.8	0xfa62	Standard query (0)	msn.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:22:52.188752890 CEST	192.168.2.7	8.8.8.8	0x21b3	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 11, 2021 22:22:54.283799887 CEST	192.168.2.7	8.8.8.8	0x652b	Standard query (0)	msn.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:22:56.114062071 CEST	192.168.2.7	8.8.8.8	0x88d0	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:15.218827963 CEST	192.168.2.7	8.8.8.8	0x405b	Standard query (0)	breuranel.website	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:16.769084930 CEST	192.168.2.7	8.8.8.8	0x3d59	Standard query (0)	breuranel.website	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:35.656286955 CEST	192.168.2.7	8.8.8.8	0xe9cb	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.228514910 CEST	192.168.2.7	8.8.8.8	0x8341	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.403567076 CEST	192.168.2.7	8.8.8.8	0xa1aa	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.862098932 CEST	192.168.2.7	8.8.8.8	0x7d86	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.430321932 CEST	192.168.2.7	8.8.8.8	0xf4db	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.616125107 CEST	192.168.2.7	8.8.8.8	0x2aa7	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:56.992526054 CEST	192.168.2.7	8.8.8.8	0xaf8	Standard query (0)	areuranel.website	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:57.968406916 CEST	192.168.2.7	8.8.8.8	0xbdb0	Standard query (0)	areuranel.website	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:17.221970081 CEST	192.168.2.7	8.8.8.8	0xd257	Standard query (0)	msn.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:17.684597969 CEST	192.168.2.7	8.8.8.8	0x849e	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:18.050049067 CEST	192.168.2.7	8.8.8.8	0x66d4	Standard query (0)	msn.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:18.577414036 CEST	192.168.2.7	8.8.8.8	0x1499	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:38.077528954 CEST	192.168.2.7	8.8.8.8	0xbd54	Standard query (0)	breuranel.website	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:39.034653902 CEST	192.168.2.7	8.8.8.8	0x6ab0	Standard query (0)	breuranel.website	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.291340113 CEST	192.168.2.7	8.8.8.8	0x4071	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.862272978 CEST	192.168.2.7	8.8.8.8	0xe22c	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.034205914 CEST	192.168.2.7	8.8.8.8	0xe54	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.093812943 CEST	192.168.2.7	8.8.8.8	0xa669	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.672101974 CEST	192.168.2.7	8.8.8.8	0xcaca	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.854630947 CEST	192.168.2.7	8.8.8.8	0x83b1	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 11, 2021 22:22:51.392652035 CEST	8.8.8.8	192.168.2.7	0xfa62	No error (0)	msn.com		13.82.28.61	A (IP address)	IN (0x0001)
Oct 11, 2021 22:22:52.206620932 CEST	8.8.8.8	192.168.2.7	0x21b3	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:22:54.299629927 CEST	8.8.8.8	192.168.2.7	0x652b	No error (0)	msn.com		13.82.28.61	A (IP address)	IN (0x0001)
Oct 11, 2021 22:22:56.132452011 CEST	8.8.8.8	192.168.2.7	0x88d0	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:15.239259005 CEST	8.8.8.8	192.168.2.7	0x405b	Name error (3)	breuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:16.788223982 CEST	8.8.8.8	192.168.2.7	0x3d59	Name error (3)	breuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:35.674390078 CEST	8.8.8.8	192.168.2.7	0xe9cb	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 11, 2021 22:23:35.674390078 CEST	8.8.8.8	192.168.2.7	0xe9cb	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:35.674390078 CEST	8.8.8.8	192.168.2.7	0xe9cb	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:35.674390078 CEST	8.8.8.8	192.168.2.7	0xe9cb	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:35.674390078 CEST	8.8.8.8	192.168.2.7	0xe9cb	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:35.674390078 CEST	8.8.8.8	192.168.2.7	0xe9cb	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:35.674390078 CEST	8.8.8.8	192.168.2.7	0xe9cb	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:35.674390078 CEST	8.8.8.8	192.168.2.7	0xe9cb	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.248886108 CEST	8.8.8.8	192.168.2.7	0x8341	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:36.248886108 CEST	8.8.8.8	192.168.2.7	0x8341	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:36.248886108 CEST	8.8.8.8	192.168.2.7	0x8341	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:36.248886108 CEST	8.8.8.8	192.168.2.7	0x8341	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:36.248886108 CEST	8.8.8.8	192.168.2.7	0x8341	No error (0)	HHN-efz.ms-acdc.office.com		40.101.91.82	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.248886108 CEST	8.8.8.8	192.168.2.7	0x8341	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.242	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.248886108 CEST	8.8.8.8	192.168.2.7	0x8341	No error (0)	HHN-efz.ms-acdc.office.com		52.97.149.82	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.248886108 CEST	8.8.8.8	192.168.2.7	0x8341	No error (0)	HHN-efz.ms-acdc.office.com		40.101.61.114	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.421677113 CEST	8.8.8.8	192.168.2.7	0xa1aa	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:36.421677113 CEST	8.8.8.8	192.168.2.7	0xa1aa	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:36.421677113 CEST	8.8.8.8	192.168.2.7	0xa1aa	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:36.421677113 CEST	8.8.8.8	192.168.2.7	0xa1aa	No error (0)	HHN-efz.ms-acdc.office.com		52.97.183.162	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.421677113 CEST	8.8.8.8	192.168.2.7	0xa1aa	No error (0)	HHN-efz.ms-acdc.office.com		52.98.208.66	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.421677113 CEST	8.8.8.8	192.168.2.7	0xa1aa	No error (0)	HHN-efz.ms-acdc.office.com		52.98.214.82	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.421677113 CEST	8.8.8.8	192.168.2.7	0xa1aa	No error (0)	HHN-efz.ms-acdc.office.com		40.101.60.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.879776955 CEST	8.8.8.8	192.168.2.7	0x7d86	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.879776955 CEST	8.8.8.8	192.168.2.7	0x7d86	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.879776955 CEST	8.8.8.8	192.168.2.7	0x7d86	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.879776955 CEST	8.8.8.8	192.168.2.7	0x7d86	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 11, 2021 22:23:36.879776955 CEST	8.8.8.8	192.168.2.7	0x7d86	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.879776955 CEST	8.8.8.8	192.168.2.7	0x7d86	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.879776955 CEST	8.8.8.8	192.168.2.7	0x7d86	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:36.879776955 CEST	8.8.8.8	192.168.2.7	0x7d86	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.448506117 CEST	8.8.8.8	192.168.2.7	0xf4db	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:37.448506117 CEST	8.8.8.8	192.168.2.7	0xf4db	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:37.448506117 CEST	8.8.8.8	192.168.2.7	0xf4db	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:37.448506117 CEST	8.8.8.8	192.168.2.7	0xf4db	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:37.448506117 CEST	8.8.8.8	192.168.2.7	0xf4db	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.114	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.448506117 CEST	8.8.8.8	192.168.2.7	0xf4db	No error (0)	HHN-efz.ms-acdc.office.com		52.97.149.242	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.448506117 CEST	8.8.8.8	192.168.2.7	0xf4db	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.162	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.448506117 CEST	8.8.8.8	192.168.2.7	0xf4db	No error (0)	HHN-efz.ms-acdc.office.com		52.97.218.82	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.634171009 CEST	8.8.8.8	192.168.2.7	0x2aa7	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:37.634171009 CEST	8.8.8.8	192.168.2.7	0x2aa7	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:37.634171009 CEST	8.8.8.8	192.168.2.7	0x2aa7	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:23:37.634171009 CEST	8.8.8.8	192.168.2.7	0x2aa7	No error (0)	HHN-efz.ms-acdc.office.com		52.97.183.162	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.634171009 CEST	8.8.8.8	192.168.2.7	0x2aa7	No error (0)	HHN-efz.ms-acdc.office.com		52.98.208.66	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.634171009 CEST	8.8.8.8	192.168.2.7	0x2aa7	No error (0)	HHN-efz.ms-acdc.office.com		52.98.214.82	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:37.634171009 CEST	8.8.8.8	192.168.2.7	0x2aa7	No error (0)	HHN-efz.ms-acdc.office.com		40.101.60.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:57.015857935 CEST	8.8.8.8	192.168.2.7	0xaf8	Name error (3)	areuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 11, 2021 22:23:57.989510059 CEST	8.8.8.8	192.168.2.7	0xbdb0	Name error (3)	areuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:17.239850998 CEST	8.8.8.8	192.168.2.7	0xd257	No error (0)	msn.com		13.82.28.61	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:17.705154896 CEST	8.8.8.8	192.168.2.7	0x849e	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:18.066231012 CEST	8.8.8.8	192.168.2.7	0x66d4	No error (0)	msn.com		13.82.28.61	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:18.595428944 CEST	8.8.8.8	192.168.2.7	0x1499	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:38.098494053 CEST	8.8.8.8	192.168.2.7	0xbd54	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 11, 2021 22:24:39.052957058 CEST	8.8.8.8	192.168.2.7	0x6ab0	Name error (3)	breuranel.website	none	none	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.309329033 CEST	8.8.8.8	192.168.2.7	0x4071	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.309329033 CEST	8.8.8.8	192.168.2.7	0x4071	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.309329033 CEST	8.8.8.8	192.168.2.7	0x4071	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.309329033 CEST	8.8.8.8	192.168.2.7	0x4071	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.309329033 CEST	8.8.8.8	192.168.2.7	0x4071	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.309329033 CEST	8.8.8.8	192.168.2.7	0x4071	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.309329033 CEST	8.8.8.8	192.168.2.7	0x4071	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.309329033 CEST	8.8.8.8	192.168.2.7	0x4071	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.881478071 CEST	8.8.8.8	192.168.2.7	0xe22c	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:58.881478071 CEST	8.8.8.8	192.168.2.7	0xe22c	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:58.881478071 CEST	8.8.8.8	192.168.2.7	0xe22c	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:58.881478071 CEST	8.8.8.8	192.168.2.7	0xe22c	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:58.881478071 CEST	8.8.8.8	192.168.2.7	0xe22c	No error (0)	HHN-efz.ms-acdc.office.com		52.97.137.178	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.881478071 CEST	8.8.8.8	192.168.2.7	0xe22c	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.114	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.881478071 CEST	8.8.8.8	192.168.2.7	0xe22c	No error (0)	HHN-efz.ms-acdc.office.com		40.101.60.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:58.881478071 CEST	8.8.8.8	192.168.2.7	0xe22c	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.50	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.054173946 CEST	8.8.8.8	192.168.2.7	0xe54	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.054173946 CEST	8.8.8.8	192.168.2.7	0xe54	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.054173946 CEST	8.8.8.8	192.168.2.7	0xe54	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.054173946 CEST	8.8.8.8	192.168.2.7	0xe54	No error (0)	FRA-efz.ms-acdc.office.com		52.97.151.18	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.054173946 CEST	8.8.8.8	192.168.2.7	0xe54	No error (0)	FRA-efz.ms-acdc.office.com		52.97.147.178	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.054173946 CEST	8.8.8.8	192.168.2.7	0xe54	No error (0)	FRA-efz.ms-acdc.office.com		52.97.212.34	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.111654997 CEST	8.8.8.8	192.168.2.7	0xa669	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.111654997 CEST	8.8.8.8	192.168.2.7	0xa669	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.111654997 CEST	8.8.8.8	192.168.2.7	0xa669	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 11, 2021 22:24:59.111654997 CEST	8.8.8.8	192.168.2.7	0xa669	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.111654997 CEST	8.8.8.8	192.168.2.7	0xa669	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.111654997 CEST	8.8.8.8	192.168.2.7	0xa669	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.111654997 CEST	8.8.8.8	192.168.2.7	0xa669	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.111654997 CEST	8.8.8.8	192.168.2.7	0xa669	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.695882082 CEST	8.8.8.8	192.168.2.7	0xcaca	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.695882082 CEST	8.8.8.8	192.168.2.7	0xcaca	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.695882082 CEST	8.8.8.8	192.168.2.7	0xcaca	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.695882082 CEST	8.8.8.8	192.168.2.7	0xcaca	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.695882082 CEST	8.8.8.8	192.168.2.7	0xcaca	No error (0)	HHN-efz.ms-acdc.office.com		40.101.60.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.695882082 CEST	8.8.8.8	192.168.2.7	0xcaca	No error (0)	HHN-efz.ms-acdc.office.com		52.97.157.162	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.695882082 CEST	8.8.8.8	192.168.2.7	0xcaca	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.146	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.695882082 CEST	8.8.8.8	192.168.2.7	0xcaca	No error (0)	HHN-efz.ms-acdc.office.com		52.97.151.2	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.875370026 CEST	8.8.8.8	192.168.2.7	0x83b1	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.875370026 CEST	8.8.8.8	192.168.2.7	0x83b1	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.875370026 CEST	8.8.8.8	192.168.2.7	0x83b1	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
Oct 11, 2021 22:24:59.875370026 CEST	8.8.8.8	192.168.2.7	0x83b1	No error (0)	FRA-efz.ms-acdc.office.com		52.97.151.18	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.875370026 CEST	8.8.8.8	192.168.2.7	0x83b1	No error (0)	FRA-efz.ms-acdc.office.com		52.97.147.178	A (IP address)	IN (0x0001)
Oct 11, 2021 22:24:59.875370026 CEST	8.8.8.8	192.168.2.7	0x83b1	No error (0)	FRA-efz.ms-acdc.office.com		52.97.212.34	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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49747	13.82.28.61	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:22:52 UTC	0	OUT	GET /mail/liopolo/XqCHqVDXW8CZUpeu5peN_2/FydjgYTJtTmoC/fAo34oef/chWHLvpFFUOYdiWXbNbnYW0/Rfy3HU21P_/2FwjKpEqeFo_2FxU6/0A_2BR4J2MVl/hx12NRqsjmC/kkNl1wduKuFf8Q/FUG3Ocqqzs1x_2BibuPx6/9auuC1P5josci_2B/vyxmzUWJ7gSzOqo/Jt7rxzWzdI7AYIGNrQ/e7oR22vyh/Me9W1V8u/5SwAx9Su/B.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 20:22:52 UTC	0	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.msn.com/mail/liopolo/XqCHqVDXW8CZUpeu5peN_2/FydjgYTJtTmoC/fAo34oef/chWHLvpFFUOYdiWXbNbnYW0/Rfy3HU21P_/2FwjKpEqeFo_2FxU6/0A_2BR4J2MVl/hx12NRqsjmC/kkNl1wduKuFf8Q/FUG3Ocqqzs1x_2BibuPx6/9auuC1P5josci_2B/vyxmzUWJ7gSzOqo/Jt7rxzWzdI7AYIGNrQ/e7oR22vyh/Me9W1V8u/5SwAx9Su/B.jre Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Date: Mon, 11 Oct 2021 20:22:51 GMT Connection: close Content-Length: 402
2021-10-11 20:22:52 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 58 71 43 48 71 56 44 58 57 38 43 5a 55 70 65 75 35 70 65 4e 5f 32 2f 46 79 64 6a 67 59 54 4a 74 54 6d 6f 43 2f 66 41 6f 33 34 6f 65 66 2f 63 68 57 48 4c 76 70 46 46 55 4f 59 64 69 57 58 62 4e 62 6e 59 57 30 2f 52 66 79 33 48 55 32 31 50 5f 2f 32 46 77 6a 4b 70 45 71 65 46 6f 5f 32 46 78 55 36 2f 30 41 5f 32 42 52 34 4a 32 4d 56 6c 2f 68 78 31 32 Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.msn.com/mail/liopolo/XqCHqVDXW8CZUpeu5peN_2/FydjgYTJtTmoC/fAo34oef/chWHLvpFFUOYdiWXbNbnYW0/Rfy3HU21P_/2FwjKpEqeFo_2FxU6/0A_2BR4J2MVl/hx12

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49749	13.82.28.61	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:22:55 UTC	1	OUT	GET /mail/liopolo/yn_2BPYQmJ20vgPRL3/3wjWE1bwH/DDPf_2FmyfN4qjiroAKh/7sxv413IrGA7KcA9Hu0/BYfxtbSdLKzFinzGkJGdmk/P_2Fifx7koRFQ/MIG6rk6P/jRWWDjWjz87k5xmFJxsJqsu/JDVOEV0_2F/rb6v_2FY3MQLb6_2F/gkDS2luFhYah/H5Mm0Y9iZUr/9_2FNXlrb5xId9/cAon_2FllX9wfUzSs9jRy/iECEQNsAU7oK/0.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 20:22:56 UTC	1	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.msn.com/mail/liopolo/yn_2BPYQmJ20vgPRL3/3wjWE1bwH/DDPf_2FmyfN4qjiroAKh/7sxv413IrGA7KcA9Hu0/BYfxtbSdLKzFinzGkJGdmk/P_2Fifx7koRFQ/MIG6rk6P/jRWWDjWjz87k5xmFJxsJqsu/JDVOEV0_2F/rb6v_2FY3MQLb6_2F/gkDS2luFhYah/H5Mm0Y9iZUr/9_2FNXlrb5xId9/cAon_2FllX9wfUzSs9jRy/iECEQNsAU7oK/0.jre Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Date: Mon, 11 Oct 2021 20:22:55 GMT Connection: close Content-Length: 405
2021-10-11 20:22:56 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 79 6e 5f 32 42 50 59 51 6d 4a 32 30 76 67 50 52 4c 33 2f 33 77 6a 57 45 31 62 77 48 2f 44 44 50 66 5f 32 46 6d 79 66 4e 34 71 6a 69 72 6f 41 4b 68 2f 37 73 78 76 34 31 33 49 72 47 41 37 4b 63 41 39 48 75 30 2f 42 59 66 78 74 62 53 64 4c 4b 7a 46 69 6e 7a 47 6b 4a 47 64 6d 6b 2f 50 5f 32 46 69 66 78 37 6b 6f 52 46 51 2f 4d 49 47 36 72 6b 36 50 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/yn_2BPYQmJ20vgPRL3/3wjWE1bwH/DDPf_2FmyfN4qjiroAKh/7sxv413IrGA7KcA9Hu0/BYfxtbSdLKzFinzGkJGdmk/P_2Fifx7koRFQ/MIG6rk6P/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.7	49836	40.97.164.146	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:24:58 UTC	14	OUT	GET /signup/liopolo/5R03kGEb4YkHyvd/vrgMCXbUCWgL9mS74E/ZNV_2FT7r/A0OAE579SB7Hx3A4JeNe/QST70In3HBC_2F_2Flg/hEE1oqV04Tcb_2BXZ4DwC_/2BDjxaFgiu1Kq/cZhA7baN/ystZ_2FV5yPDIe8qQfN_2Fy/gQ02q5YT1n/eawFPHFBcfhAYskcF/Z0kyVxsdmmeN/mzjXdayEo/OIVTn_2Fwlw/Fu.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 20:24:58 UTC	15	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/signup/liopolo/5R03kGEb4YkHyvd/vrgMCXbUCWgL9mS74E/ZNV_2FT7r/A0OAE579SB7Hx3A4JeNe/QST70In3HBC_2F_2Flg/hEE1oqV04Tcb_2BXZ4DwC_/2BDjxaFgiu1Kq/cZhA7baN/ystZ_2FV5yPDIe8qQfN_2Fy/gQ02q5YT1n/eawFPHFBcfhAYskcF/Z0kyVxsdmmeN/mzjXdayEo/OIVTn_2Fwlw/Fu.jre Server: Microsoft-IIS/10.0 request-id: 8099a53e-65af-3880-089e-cf2445712a7f Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: DM5PR12CA0067 X-RequestId: 550a032f-ef09-4904-8e85-4a39f2296aff MS-CV: PqWZgK9lgDgIns8kRXEqfw.0 X-Powered-By: ASP.NET X-FEServer: DM5PR12CA0067 Date: Mon, 11 Oct 2021 20:24:57 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.7	49837	52.97.137.178	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:24:58 UTC	15	OUT	GET /signup/liopolo/5R03kGEb4YkHyvd/vrgMCXbUCWgL9mS74E/ZNV_2FT7r/A0OAE579SB7Hx3A4JeNe/QST70In3HBC_2F_2Flg/hEE1oqV04Tcb_2BXZ4DwC_/2BDjxaFgiu1Kq/cZhA7baN/ystZ_2FV5yPDIe8qQfN_2Fy/gQ02q5YT1n/eawFPHFBcfhAYskcF/Z0kyVxsdmmeN/mzjXdayEo/OIVTn_2Fwlw/Fu.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 20:24:59 UTC	16	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/signup/liopolo/5R03kGEb4YkHyvd/vrgMCXbUCWgL9mS74E/ZNV_2FT7r/A0OAE579SB7Hx3A4JeNe/QST70In3HBC_2F_2Flg/hEE1oqV04Tcb_2BXZ4DwC_/2BDjxaFgiu1Kq/cZhA7baN/ystZ_2FV5yPDIe8qQfN_2Fy/gQ02q5YT1n/eawFPHFBcfhAYskcF/Z0kyVxsdmmeN/mzjXdayEo/OIVTn_2Fwlw/Fu.jre Server: Microsoft-IIS/10.0 request-id: b9b7327e-5b78-5b44-ef43-2c8ec9713b98 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AM6P192CA0067 X-RequestId: f30f3fcf-a4dd-4657-ad11-fef223c73bd5 MS-CV: fjK3uXhbRFvvQyyOyXE7mA.0 X-Powered-By: ASP.NET X-FEServer: AM6P192CA0067 Date: Mon, 11 Oct 2021 20:24:58 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.7	49838	52.97.151.18	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:24:59 UTC	16	OUT	GET /signup/liopolo/5R03kGEb4YkHyvd/vrgMCXbUCWgL9mS74E/ZNV_2FT7r/A0OAE579SB7Hx3A4JeNe/QST70In3HBC_2F_2Flg/hEE1oqV04Tcb_2BXZ4DwC_/2BDjxaFgiu1Kq/cZhA7baN/ystZ_2FV5yPDIe8qQfN_2Fy/gQ02q5YT1n/eawFPHFBcfhAYskcF/Z0kyVxsdmmeN/mzjXdayEo/OIVTn_2Fwlw/Fu.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 20:24:59 UTC	17	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: de37bbb0-742b-37a2-87bd-bd1fca420c34 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: HE1PR05CU010.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: HE1PR05CA0294.EURPRD05.PROD.OUTLOOK.COM X-CalculatedBETarget: HE1P193MB0009.EURP193.PROD.OUTLOOK.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: sLs33it0ojeHvb0fykIMNA.1.1 X-FEServer: HE1PR05CA0294 X-Powered-By: ASP.NET X-FEServer: AM6P193CA0092 Date: Mon, 11 Oct 2021 20:24:58 GMT Connection: close
2021-10-11 20:24:59 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 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
13	192.168.2.7	49839	40.97.164.146	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:24:59 UTC	19	OUT	GET /signup/liopolo/7RiyOegViATthNX4pt/E65VkdFK0/peIG_2BaG1SxNKYOcdXs/80APf88JeQpK_2BfrxB/1_2B2_2FNDAEnuSdYMUmdr/BpxBwvlUzTu3W/v3tDiaIH/uhnULhLXCDfDONp_2FCc03F/ZkPsDATWsR/KNPTfNdkqqbWMwLBy/xU_2Bk46LKIT/9_2FOKzik9g/v8mZTndKcyg89a/ELxzR_2BALqku0rQMRn2U/KVAF7ruVq/mnKq.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 20:24:59 UTC	19	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/signup/liopolo/7RiyOegViATthNX4pt/E65VkdFK0/peIG_2BaG1SxNKYOcdXs/80APf88JeQpK_2BfrxB/1_2B2_2FNDAEnuSdYMUmdr/BpxBwvlUzTu3W/v3tDiaIH/uhnULhLXCDfDONp_2FCc03F/ZkPsDATWsR/KNPTfNdkqqbWMwLBy/xU_2Bk46LKIT/9_2FOKzik9g/v8mZTndKcyg89a/ELxzR_2BALqku0rQMRn2U/KVAF7ruVq/mnKq.jre Server: Microsoft-IIS/10.0 request-id: 1e93f8c3-830c-1ea8-5c43-4416fe7d809a Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: DM5PR12CA0049 X-RequestId: 3b392557-e5a2-404f-b4de-d23d99694827 MS-CV: w/iTHgyDqB5cQ0QW/n2Amg.0 X-Powered-By: ASP.NET X-FEServer: DM5PR12CA0049 Date: Mon, 11 Oct 2021 20:24:59 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.7	49840	40.101.60.2	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:24:59 UTC	20	OUT	GET /signup/liopolo/7RiyOegViATthNX4pt/E65VkdFK0/peIG_2BaG1SxNKYOcdXs/80APf88JeQpK_2BfrxB/1_2B2_2FNDAEnuSdYMUmdr/BpxBwvlUzTu3W/v3tDiaIH/uhnULhLXCDfDONp_2FCc03F/ZkPsDATWsR/KNPTfNdkqqbWMwLBy/xU_2Bk46LKIT/9_2FOKzik9g/v8mZTndKcyg89a/ELxzR_2BALqku0rQMRn2U/KVAF7ruVq/mnKq.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 20:24:59 UTC	20	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/signup/liopolo/7RiyOegViATthNX4pt/E65VkdFK0/peIG_2BaG1SxNKYOcdXs/80APf88JeQpK_2BfrxB/1_2B2_2FNDAEnuSdYMUmdr/BpxBwvlUzTu3W/v3tDiaIH/uhnULhLXCDfDONp_2FCc03F/ZkPsDATWsR/KNPTfNdkqqbWMwLBy/xU_2Bk46LKIT/9_2FOKzik9g/v8mZTndKcyg89a/ELxzR_2BALqku0rQMRn2U/KVAF7ruVq/mnKq.jre Server: Microsoft-IIS/10.0 request-id: 08857e56-471f-5dd0-62e1-55fcf4807e17 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AM5PR0601CA0033 X-RequestId: a944b9ab-d067-4189-87b9-0baccc96b6f7 MS-CV: Vn6FCB9H0F1i4VX89IB+Fw.0 X-Powered-By: ASP.NET X-FEServer: AM5PR0601CA0033 Date: Mon, 11 Oct 2021 20:24:59 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.7	49841	52.97.151.18	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:24:59 UTC	21	OUT	GET /signup/liopolo/7RiyOegViATthNX4pt/E65VkdFK0/peIG_2BaG1SxNKYOcdXs/80APf88JeQpK_2BfrxB/1_2B2_2FNDAEnuSdYMUmdr/BpxBwvlUzTu3W/v3tDiaIH/uhnULhLXCDfDONp_2FCc03F/ZkPsDATWsR/KNPTfNdkqqbWMwLBy/xU_2Bk46LKIT/9_2FOKzik9g/v8mZTndKcyg89a/ELxzR_2BALqku0rQMRn2U/KVAF7ruVq/mnKq.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 20:25:00 UTC	21	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: cc782159-69ef-cf03-4f21-5a1c9fd141af Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: VI1PR06CU004.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: VI1PR06CA0144.EURPRD06.PROD.OUTLOOK.COM X-CalculatedBETarget: VI1P193MB0047.EURP193.PROD.OUTLOOK.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: WSF4zO9pA89PIVocn9FBrw.1.1 X-FEServer: VI1PR06CA0144 X-Powered-By: ASP.NET X-FEServer: AM6P193CA0101 Date: Mon, 11 Oct 2021 20:25:00 GMT Connection: close
2021-10-11 20:25:00 UTC	22	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	192.168.2.7	49762	40.97.164.146	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:23:36 UTC	2	OUT	GET /signup/liopolo/yxX7bEpX8fkEJbVyh9/qWpi3f2OW/wrbjI8c5A6cpHeOUtqJL/SsvBBOkr1Vxt3lBY9zj/5j0TGmFjnVfmYPqQrqQKOy/CuHlAfsl6J0Xl/Gz8IEoLZ/BwAkxXP5B5W2_2BPU7pGqQ9/BHC7nncuP2/eu0pY6BQJ958LuV7l/fzySs8nJ5lF3/1CG1ppCNJBl/xHTFfKCof0ib7S/py_2F4IYCav_2Ftxe98nI/nZH.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 20:23:36 UTC	3	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/signup/liopolo/yxX7bEpX8fkEJbVyh9/qWpi3f2OW/wrbjI8c5A6cpHeOUtqJL/S svBBOkr1Vxt3lBY9zj/5j0TGmFjnVfmYPqQrqQKOy/CuHlAfsl6J0Xl/Gz8IEoLZ/BwAkxXP5B5W2_2BPU7pGqQ9/B HC7nncuP2/eu0pY6BQJ958LuV7I/fzySs8nJ5lF3/1CG1ppCNJBl/xHTFfKCof0ib7S/py_2F4IYCav_2Ftxe98nl/nZH.jre Server: Microsoft-IIS/10.0 request-id: 6d1b24da-1cc8-ee3a-1519-89c9b908c7bd Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: DM5PR12CA0059 X-RequestId: d1ffad17-cc5f-4b5d-b74b-6b7051898e88 MS-CV: 2iQbbcgcOu4VGYnJuQjHvQ.0 X-Powered-By: ASP.NET X-FEServer: DM5PR12CA0059 Date: Mon, 11 Oct 2021 20:23:36 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49763	40.101.91.82	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:23:36 UTC	3	OUT	GET /signup/liopolo/yxX7bEpX8fkEJbVyh9/qWpi3f2OW/wrbjI8c5A6cpHeOUtqJL/SsvBBOkr1Vxt3lBY9zj/5j0TGmFjnV fmYPqQrqQKOy/CuHlAfsl6J0Xl/Gz8IEoLZ/BwAkxXP5B5W2_2BPU7pGqQ9/BHC7nncuP2/eu0pY6BQJ958LuV7I/f zySs8nJ5lF3/1CG1ppCNJBl/xHTFfKCof0ib7S/py_2F4IYCav_2Ftxe98nl/nZH.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 20:23:36 UTC	4	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/signup/liopolo/yxX7bEpX8fkEJbVyh9/qWpi3f2OW/wrbjI8c5A6cpHeOUtqJL/SsvBB Okr1Vxt3lBY9zj/5j0TGmFjnVfmYPqQrqQKOy/CuHlAfsl6J0Xl/Gz8IEoLZ/BwAkxXP5B5W2_2BPU7pGqQ9/BHC7n ncuP2/eu0pY6BQJ958LuV7I/fzySs8nJ5lF3/1CG1ppCNJBl/xHTFfKCof0ib7S/py_2F4IYCav_2Ftxe98nl/nZH.jre Server: Microsoft-IIS/10.0 request-id: f7569adb-4650-dae2-9c11-70866ed53d1f Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AM6PR10CA0038 X-RequestId: 462b7eda-63f1-4417-bdce-c932f36b8bb1 MS-CV: 25pW91BG4tqcEXCGbtU9Hw.0 X-Powered-By: ASP.NET X-FEServer: AM6PR10CA0038 Date: Mon, 11 Oct 2021 20:23:36 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49764	52.97.183.162	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:23:36 UTC	5	OUT	GET /signup/liopolo/yxX7bEpX8fkEJbVyh9/qWpi3f2OW/wrbjI8c5A6cpHeOUtqJL/SsvBBOkr1Vxt3lBY9zj/5j0TGmFjnV fmYPqQrqQKOy/CuHlAfsl6J0Xl/Gz8IEoLZ/BwAkxXP5B5W2_2BPU7pGqQ9/BHC7nncuP2/eu0pY6BQJ958LuV7I/f zySs8nJ5lF3/1CG1ppCNJBl/xHTFfKCof0ib7S/py_2F4IYCav_2Ftxe98nl/nZH.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 20:23:36 UTC	5	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: 4a6581a2-619b-52fc-a3a1-1b46c2d11731 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: AM0PR02CU005.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: AM0PR02CA0158.EURPRD02.PROD.OUTLOOK.COM X-CalculatedBETarget: AM0PR0302MB3315.eurprd03.prod.outlook.com X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: ooFlSpth/FKjoRtGwtEXMQ.1.1 X-FEServer: AM0PR02CA0158 X-Powered-By: ASP.NET X-FEServer: AM7PR03CA0005 Date: Mon, 11 Oct 2021 20:23:36 GMT Connection: close
2021-10-11 20:23:36 UTC	6	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	192.168.2.7	49765	40.97.164.146	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:23:37 UTC	7	OUT	GET /signup/liopolo/f5kvQFsIv4wED/j69h8mSZ/xzzTxsSNNb1pIF2nd0zyLKL/oW0UsUUi2h/1n_2FrPb8KlH0Zm6I/DMN_2B2Rb3dP/VgvW0BFn0fE/SZJzWGdiy3m5qM/ymewVR1TpC9Ou3wlV9Okm/omWH_2FxfhHZzw96/HP0eihm9FW1uN9V/ykWA9NBBnDVcWXTKfE/JwgC0Jx4CafbQ/qgLsjM_2/F.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 20:23:37 UTC	7	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://www.outlook.com/signup/liopolo/f5kvQFsIv4wED/j69h8mSZ/xzzTxsSNNb1pIF2nd0zyLKL/oW0UsUUi2h/1n_2FrPb8KlH0Zm6I/DMN_2B2Rb3dP/VgvW0BFn0fE/SZJzWGdiy3m5qM/ymewVR1TpC9Ou3wlV9Okm/omWH_2FxfhHZzw96/HP0eihm9FW1uN9V/ykWA9NBBnDVcWXTKfE/JwgC0Jx4CafbQ/qgLsjM_2/F.jre Server: Microsoft-IIS/10.0 request-id: d574ae41-5ffa-a7f2-a157-9e14ff00da45 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: DM5PR12CA0059 X-RequestId: 610fa43b-ed9f-41be-a771-e616baf7de16 MS-CV: Qa501fpf8qehV54U/wDaRQ.0 X-Powered-By: ASP.NET X-FEServer: DM5PR12CA0059 Date: Mon, 11 Oct 2021 20:23:37 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49766	52.97.151.114	443	C:\Windows\System32\loaddll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:23:37 UTC	8	OUT	GET /signup/liopolo/f5kvQFsIv4wED/j69h8mSZ/xzzTxsSNNb1pIF2nd0zyLKL/oW0UsUUi2h/1n_2FrPb8KlH0Zm6I/DMN_2B2Rb3dP/VgvW0BFn0fE/SZJzWGdiy3m5qM/ymewVR1TpC9Ou3wlV9Okm/omWH_2FxfhHZzw96/HP0eihm9FW1uN9V/ykWA9NBBnDVcWXTKfE/JwgC0Jx4CafbQ/qgLsjM_2/F.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 20:23:37 UTC	8	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.office365.com/signup/liopolo/f5kvQFsIv4wED/j69h8mSZ/xzzTxsSNNb1pIF2nd0zyLKL/oW0UsUUi2h/1n_2FrPb8KlH0Zm6I/DMN_2B2Rb3dP/VgvW0BFn0fE/SZJzWGdiy3m5qM/ymewVR1TpC9Ou3wlV9Okm/omWH_2FxfhHZzw96/HP0eihm9FW1uN9V/ykWA9NBBnDVcWXTKfE/JwgC0Jx4CafbQ/qgLsjM_2/F.jre Server: Microsoft-IIS/10.0 request-id: d4464c06-3114-7586-23c3-25ff50d01eb3 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-FEServer: AM6P193CA0066 X-RequestId: 400f9696-6aba-4248-82af-0dd429669fdb MS-CV: BkxG1BQxhnUjwyX/UNAesw.0 X-Powered-By: ASP.NET X-FEServer: AM6P193CA0066 Date: Mon, 11 Oct 2021 20:23:36 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49767	52.97.183.162	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:23:37 UTC	9	OUT	GET /signup/liopolo/f5kvQFsIv4wED/j69h8mSZ/xzzTxsSNNb1pIF2nd0zyLKL/oW0UsUUi2h/1n_2FrPb8KlH0Zm6I/DMN_2B2Rb3dP/VgvW0BFn0fE/SZJzWGdiy3m5qM/ymewVR1TpC9Ou3wlV9Okm/omWH_2FxfhHZzw96/HP0eihm9FW1uN9V/ykWA9NBBnDVcWXTKfE/JwgC0Jx4CafbQ/qgLsjM_2/F.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 20:23:37 UTC	9	IN	HTTP/1.1 404 Not Found Content-Length: 1245 Content-Type: text/html Server: Microsoft-IIS/10.0 request-id: 3d79bdb5-66ac-6d20-1236-ee020757b4df Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-CalculatedFETarget: DU2PR04CU011.internal.outlook.com X-BackEndHttpStatus: 404 X-FEProxyInfo: DU2PR04CA0330.EURPRD04.PROD.OUTLOOK.COM X-CalculatedBETarget: DB6PR03MB2838.EURPRD03.PROD.OUTLOOK.COM X-BackEndHttpStatus: 404 X-RUM-Validated: 1 X-Proxy-RoutingCorrectness: 1 X-Proxy-BackendServerStatus: 404 MS-CV: tb15PaxmIG0SNu4CB1e03w.1.1 X-FEServer: DU2PR04CA0330 X-Powered-By: ASP.NET X-FEServer: AM7PR03CA0017 Date: Mon, 11 Oct 2021 20:23:37 GMT Connection: close
2021-10-11 20:23:37 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 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	192.168.2.7	49810	13.82.28.61	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:24:17 UTC	11	OUT	GET /mail/liopolo/A1Qp_2BWzai2O5/xac_2BRG3wzSiIIBjQnWR/yH8MK_2FDeyVZ7zs/MmgvT5kbS5J14SI/50tiJJe1m8aJQ2XT7T/rIRQt7iCb/CwoKyLq7nfSWQHvgpN7o/BCyQHF5XZOebluFzT_2/BFFOtw4QHhKTLswkkvF9vD/aY9DT6JVICQxS/piqcZUHz/pQlXCrwUL0BTmEd_2FLWL2L/RH2uj8PySJ/d2LKLIyBddk3_2FhT/H.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 20:24:17 UTC	12	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.msn.com/mail/liopolo/A1Qp_2BWzai2O5/xac_2BRG3wzSilIBjQnWR/yH8MK_2FDeyVZ7zs/MmgvT5kbS5J14SI/50tiJJe1m8aJQ2XT7T/rIRQt7iCb/CwoKyLq7nfSWQHvgpN7o/BCyQHF5XZOebluFzT_2/BFFOtw4QHhKTLswkkvF9vD/aY9DT6JVICQxS/piqcZUHz/pQlXCrwUL0BTmEd_2FLWL2L/RH2uj8PySJ/d2LKLlyBddk3_2FhT/H.jre Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Date: Mon, 11 Oct 2021 20:24:17 GMT Connection: close Content-Length: 400
2021-10-11 20:24:17 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 41 31 51 70 5f 32 42 57 7a 61 69 32 4f 35 2f 78 61 63 5f 32 42 52 47 33 77 7a 53 69 6c 49 42 6a 51 6e 57 52 2f 79 48 38 4d 4b 5f 32 46 44 65 79 56 5a 37 7a 73 2f 4d 6d 67 76 54 35 6b 62 53 35 4a 31 34 53 49 2f 35 30 74 69 4a 4a 65 31 6d 38 61 4a 51 32 58 54 37 54 2f 72 49 52 51 74 37 69 43 62 2f 43 77 6f 4b 79 4c 71 37 6e 66 53 57 51 48 76 67 70 Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.msn.com/mail/liopolo/A1Qp_2BWzai2O5/xac_2BRG3wzSilIBjQnWR/yH8MK_2FDeyVZ7zs/MmgvT5kbS5J14SI/50tiJJe1m8aJQ2XT7T/rIRQt7iCb/CwoKyLq7nfSWQHvgp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.7	49815	13.82.28.61	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-11 20:24:18 UTC	13	OUT	GET /mail/liopolo/pf6_2FLREfP_2FxP/xGe8YUjshftOGCf/JTttK9QVtKrTS7QkWE/ZPLHtzaUx/XGEoZcanWnYYYh5pU8Em/GLDLy5GpGXwcg_2Bwck/kT4Zd7sERIG_2Bba1DdBVT/1BoxASA_2FDOZ/PsNxvKNH/RweAmXaL_2B7o4rtkWRlTX9/6ZU5YSIMnk/yFSTinelYwomOZkWD/rkossiVbXA0U/C_2FCIlnEO_/2FzjQ_2By_2FPmxqq/uw86.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 20:24:18 UTC	13	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.msn.com/mail/liopolo/pf6_2FLREfP_2FxP/xGe8YUjshftOGCf/JTttK9QVtKrTS7QkWE/ZPLHtzaUx/XGEoZcanWnYYYh5pU8Em/GLDLy5GpGXwcg_2Bwck/kT4Zd7sERIG_2Bba1DdBVT/1BoxASA_2FDOZ/PsNxvKNH/RweAmXaL_2B7o4rtkWRlTX9/6ZU5YSIMnk/yFSTinelYwomOZkWD/rkossiVbXA0U/C_2FCIlnEO_/2FzjQ_2By_2FPmxqq/uw86.jre Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Date: Mon, 11 Oct 2021 20:24:18 GMT Connection: close Content-Length: 409
2021-10-11 20:24:18 UTC	14	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 70 66 36 5f 32 46 4c 52 45 66 50 5f 32 46 78 50 2f 78 47 65 38 59 55 6a 73 68 66 74 4f 47 43 66 2f 4a 54 74 74 4b 39 51 56 74 4b 72 54 53 37 51 6b 57 45 2f 5a 50 4c 48 74 7a 61 55 78 2f 58 47 45 6f 5a 63 61 6e 57 6e 59 59 59 68 35 70 55 38 45 6d 2f 47 4c 44 4c 79 35 47 70 47 58 77 63 67 5f 32 42 77 63 6b 2f 6b 54 34 5a 64 37 73 45 52 49 47 5f 32 Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.msn.com/mail/liopolo/pf6_2FLREfP_2FxP/xGe8YUjshftOGCf/JTttK9QVtKrTS7QkWE/ZPLHtzaUx/XGEoZcanWnYYYh5pU8Em/GLDLy5GpGXwcg_2Bwck/kT4Zd7sERIG_2

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6116 Parent PID: 5632

General

Start time:	22:20:56
Start date:	11/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\B6VQd36tt6.dll'
Imagebase:	0xfc0000
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: 00000000.00000003.638534724.0000000002D1F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506367708.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.550238977.0000000002F1B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506469970.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506985927.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506632233.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506394245.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506684501.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.455038196.0000000000850000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.783361786.0000000002CA0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506547628.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506326169.0000000003098000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.783230082.0000000002B79000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.595315126.0000000002E1D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.506579239.0000000003098000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4024 Parent PID: 6116

General

Start time:	22:20:57
Start date:	11/10/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\B6VQd36tt6.dll',#1
Imagebase:	0x870000
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: 4892 Parent PID: 6116

General

Start time:	22:20:57
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\B6VQd36tt6.dll,BeGrass
Imagebase:	0x1010000
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: 00000002.00000003.418099861.0000000000A60000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4720 Parent PID: 4024

General

Start time:	22:20:57
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\B6VQd36tt6.dll',#1
Imagebase:	0x1010000
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: 00000003.00000003.499708236.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.785119761.00000000053F0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.498145572.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.419038437.0000000003030000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.500076992.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.636450090.000000000546F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.499560563.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.497950814.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.498605690.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.499306032.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.499390422.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.499160942.00000000057E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.592754619.000000000556D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.546937803.000000000566B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.784698066.0000000005039000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5780 Parent PID: 6116

General

Start time:	22:21:01
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\B6VQd36tt6.dll,Fieldeight
Imagebase:	0x1010000
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: 00000005.00000003.446200223.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 724 Parent PID: 6116

General

Start time:	22:21:08
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\B6VQd36tt6.dll,Often
Imagebase:	0x1010000
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: 00000006.00000003.452964722.0000000000D70000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 4364 Parent PID: 4892

General

Start time:	22:22:42
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4892 -s 864
Imagebase:	0x940000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WerFault.exe PID: 2836 Parent PID: 5780

General

Start time:	22:22:48
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5780 -s 840
Imagebase:	0x940000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Analysis Process: WerFault.exe PID: 4736 Parent PID: 724

General

Start time:	22:22:53
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 724 -s 636
Imagebase:	0x940000
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