ID: 679156
Sample Name: zwM7Oe2e1l
Cookbook: default.jbs
Time: 11:01:41
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

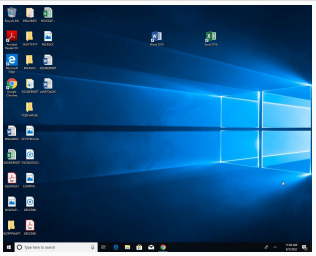
Windows Analysis Report

zwM7Oe2e1l

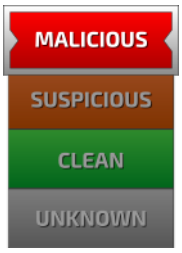
Overview

General Information

Sample Name:	zwM7Oe2e1l (renamed file extension from none to exe)
Analysis ID:	679156
MD5:	f1ab9ed37b68ac..
SHA1:	4fc5eea47502e6..
SHA256:	b65bc098b47599..
Tags:	exe WoodyRAT
Infos:	HTTP



Detection

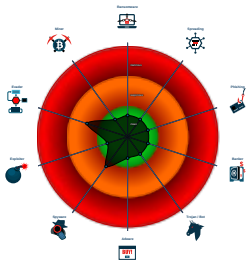


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an i…
- Snort IDS alert for network traffic
- Queries the volume information (nam…
- Sample file is different than original …
- PE file contains strange resources
- May sleep (evasive loops) to hinder…
- PE file contains sections with non-s…
- Sample execution stops while proce…
- Contains long sleeps (>= 3 min)

Classification



Process Tree

- **System is w10x64**
- zwM7Oe2e1l.exe (PID: 1316 cmdline: "C:\Users\user\Desktop\zwM7Oe2e1l.exe" MD5: F1AB9ED37B68ACE769DCCAA693F162E0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.859293532037937 08/05/22-11:02:51.521843
SID:	2037937
Source Port:	59293
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.68.8.8.855201532037937 08/05/22-11:02:51.225834
SID:	2037937
Source Port:	55201
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.68.8.8.856550532037937 08/05/22-11:02:54.471667
SID:	2037937
Source Port:	56550
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.68.8.8.856591532037937 08/05/22-11:02:52.438751
SID:	2037937
Source Port:	56591
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.68.8.8.855788532037938 08/05/22-11:04:47.473277
SID:	2037938
Source Port:	55788
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.68.8.8.861116532037937 08/05/22-11:02:53.326830
SID:	2037937
Source Port:	61116
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.68.8.8.858723532037937 08/05/22-11:02:51.809410
SID:	2037937
Source Port:	58723
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.68.8.8.863104532037938 08/05/22-11:04:09.074489
SID:	2037938
Source Port:	63104
Destination Port:	53

Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.858689532037938 08/05/22-11:03:44.188103
SID:	2037938
Source Port:	58689
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.861607532037937 08/05/22-11:02:54.097826
SID:	2037937
Source Port:	61607
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.854015532037938 08/05/22-11:03:31.447464
SID:	2037938
Source Port:	54015
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.865367532037938 08/05/22-11:04:21.925023
SID:	2037938
Source Port:	65367
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.860350532037937 08/05/22-11:02:52.686111
SID:	2037937
Source Port:	60350
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.851748532037937 08/05/22-11:02:52.976163
SID:	2037937
Source Port:	51748
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.68.8.8.859871532037938 08/05/22-11:03:07.881163
SID:	2037938
Source Port:	59871
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.851971532037937 08/05/22-11:02:52.201354
SID:	2037937
Source Port:	51971
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.851194532037938 08/05/22-11:03:18.845501
SID:	2037938
Source Port:	51194
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.857669532037938 08/05/22-11:04:34.382443
SID:	2037938
Source Port:	57669
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.850958532037937 08/05/22-11:02:53.714812
SID:	2037937
Source Port:	50958
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.852858532037938 08/05/22-11:02:54.797599
SID:	2037938
Source Port:	52858
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.853049532037938 08/05/22-11:03:56.868334
SID:	2037938
Source Port:	53049
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Networking

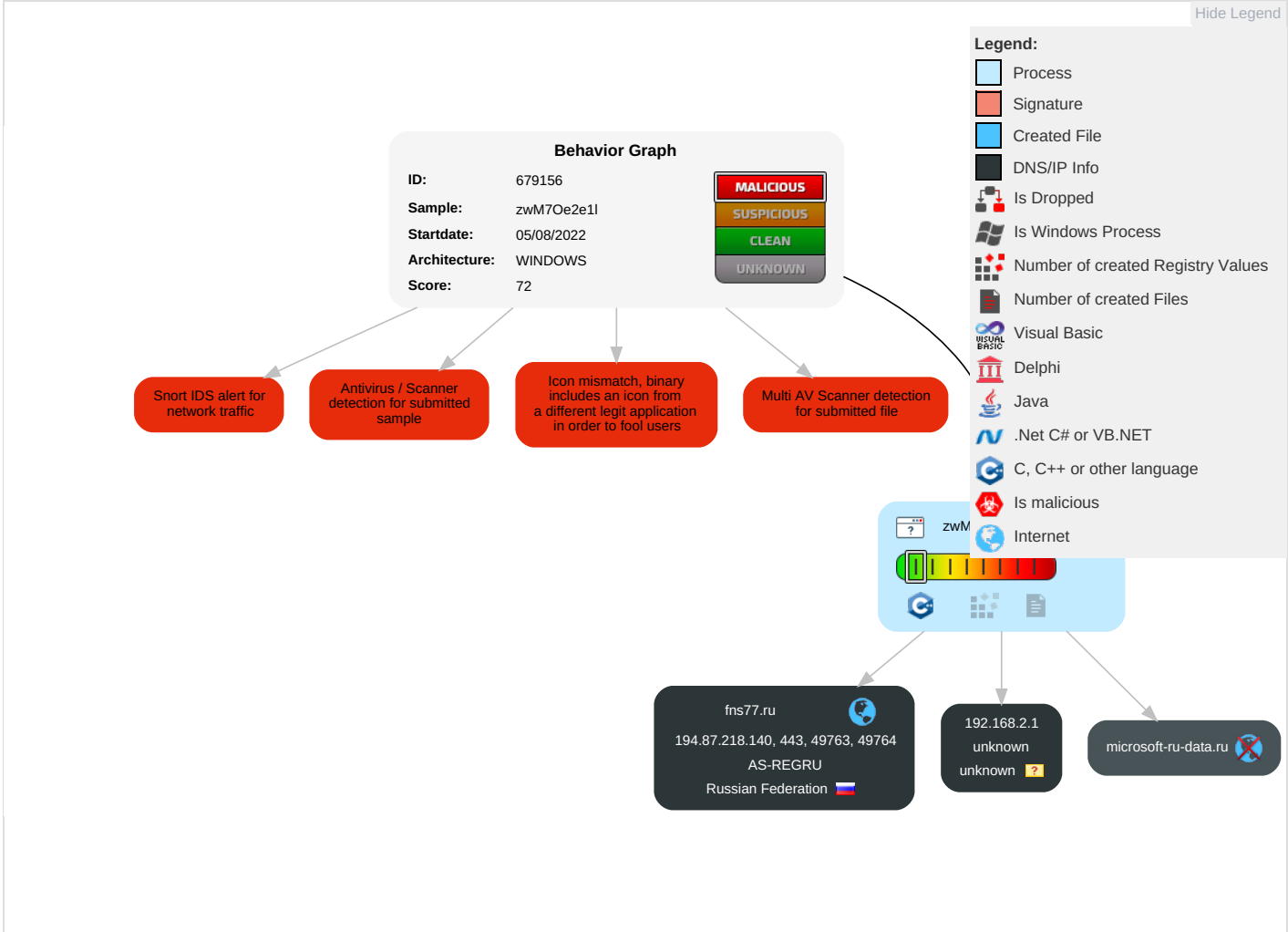
Snort IDS alert for network traffic

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

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
zwM7Oe2e1l.exe	59%	Virustotal		Browse
zwM7Oe2e1l.exe	14%	Metadefender		Browse
zwM7Oe2e1l.exe	62%	ReversingLabs	Win64.Trojan.Dothetuk	

Source	Detection	Scanner	Label	Link
zwM7Oe2e1l.exe	100%	Avira	TR/Nanocode.qtdxl	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://microsoft-ru-data.ru/knockc	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/Y	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/knockd	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/knocke	0%	Avira URL Cloud	safe	
http://https://fns77.ru/knockC3	0%	Avira URL Cloud	safe	
http://https://fns77.ru:443/knockxGO6	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/knock%)	0%	Avira URL Cloud	safe	
http://https://fns77.ru/knock	0%	Avira URL Cloud	safe	
http://https://fns77.ru/knock?.	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/ck	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/knockW	0%	Avira URL Cloud	safe	
http://https://fns77.ru/knockKkz	0%	Avira URL Cloud	safe	
http://https://fns77.ru/knock)0O	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/knockZ	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/knocks)	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/knock	0%	Avira URL Cloud	safe	
http://https://mis77.ru/	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/6	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/x	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru:443/knock	0%	Avira URL Cloud	safe	
http://https://fns77.ru/knockr	0%	Avira URL Cloud	safe	
http://https://fns77.ru/knockq	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/ckW	0%	Avira URL Cloud	safe	
http://https://fns77.ru/m	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/ckZ	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/knock#f1	0%	Avira URL Cloud	safe	
http://https://fns77.ru/e	0%	Avira URL Cloud	safe	
http://https://fns77.ru/d	0%	Avira URL Cloud	safe	
http://https://fns77.ru/	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/l	0%	Avira URL Cloud	safe	
http://https://microsoft-ru-data.ru/r	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fns77.ru	194.87.218.140	true	false		unknown
microsoft-ru-data.ru	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://microsoft-ru-data.ru/knockc	zwM7Oe2e1l.exe, 00000002.00000003.368713421.000001F180247000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/Y	zwM7Oe2e1l.exe, 00000002.00000003.367111100.000001F180247000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.369408265.000001F180247000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.366618138.000001F180247000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370201861.000001F180247000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.371162191.000001F180247000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/knockd	zwM7Oe2e1l.exe, 00000002.00000003.369394137.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.367767742.000001F180235000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/knocke	zwM7Oe2e1l.exe, 00000002.00000003.366085455.000001F180235000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru/knockC3	zwM7Oe2e1l.exe, 00000002.00000002.627362850.000001F180260000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru:443/knockxGO6	zwM7Oe2e1l.exe, 00000002.00000003.449602137.000001F180260000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476939167.000001F180268000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504317321.000001F180268000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584598044.000001F180268000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530208861.000001F180268000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/knock%)	zwM7Oe2e1l.exe, 00000002.00000003.371379761.000001F180275000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370920493.000001F180275000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fns77.ru/knock	zwM7Oe2e1l.exe, 00000002.00000003.557772748.000001F180261000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530234039.000001F180277000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504276141.000001F180261000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476801924.000001F180237000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530110478.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476883519.000001F180261000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.449653886.000001F18027F000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584585700.000001F180261000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000002.627247814.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530193276.000001F180260000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.449602137.000001F180260000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.449519735.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.399547079.000001F180280000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.422978366.000001F180281000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504027968.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584550699.000001F180237000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476964147.000001F18027B000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.449633913.000001F18027B000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000002.627020793.000001F1801EB000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504420886.000001F18027C000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584630455.000001F180277000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru/knock?.	zwM7Oe2e1l.exe, 00000002.00000003.449653886.000001F18027F000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.449633913.000001F18027B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/ck	zwM7Oe2e1l.exe, 00000002.00000003.369408265.000001F180247000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/	zwM7Oe2e1l.exe, 00000002.00000003.364691804.000001F180245000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000002.627020793.000001F1801EB000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.369036380.000001F180264000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370920493.000001F180275000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/knockW	zwM7Oe2e1l.exe, 00000002.00000003.364275197.000001F180242000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru/knockKkz	zwM7Oe2e1l.exe, 00000002.00000002.627247814.000001F180235000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru/knock)0O	zwM7Oe2e1l.exe, 00000002.00000003.584585700.000001F180261000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/knockZ	zwM7Oe2e1l.exe, 00000002.00000003.364275197.000001F180242000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://microsoft-ru-data.ru/knocks)	zwM7Oe2e1l.exe, 00000002.00000003.369320038.000001F180278000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.369901342.000001F180278000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370610227.000001F180278000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370146613.000001F180278000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370920493.000001F180275000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/knock	zwM7Oe2e1l.exe, 00000002.00000003.367781850.000001F180247000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.371141170.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.365233268.000001F180247000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.366085455.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.363930144.000001F180242000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370610227.000001F180278000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.365226384.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370146613.000001F180278000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.367767742.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.366094915.000001F180247000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370181710.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.369088197.000001F180278000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.368622773.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.367097339.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.370920493.000001F180275000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mis77.ru/	zwM7Oe2e1l.exe, 00000002.00000003.449602137.000001F180260000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476939167.000001F180268000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504317321.000001F180268000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584598044.000001F180268000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530208861.000001F180268000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/6	zwM7Oe2e1l.exe, 00000002.00000003.367111100.000001F180247000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/x	zwM7Oe2e1l.exe, 00000002.00000003.363930144.000001F180242000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.364275197.000001F180242000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.364691804.000001F180245000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru:443/knock	zwM7Oe2e1l.exe, 00000002.00000003.366020901.000001F180265000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.366905937.000001F180268000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.366530703.000001F180265000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fns77.ru/knockr	zwM7Oe2e1l.exe, 00000002.00000003.504420886.000001F18027C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru/knockq	zwM7Oe2e1l.exe, 00000002.00000003.422978366.000001F180281000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/ckW	zwM7Oe2e1l.exe, 00000002.00000003.365233268.000001F180247000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru/m	zwM7Oe2e1l.exe, 00000002.00000003.557540751.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584696071.000001F180285000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.557947549.000001F180277000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476801924.000001F180237000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530110478.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000002.627247814.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.449519735.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504027968.000001F180235000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584550699.000001F180237000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584630455.000001F180277000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/ckZ	zwM7Oe2e1l.exe, 00000002.00000003.366094915.000001F180247000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/knock#f1	zwM7Oe2e1l.exe, 00000002.00000003.365226384.000001F180235000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru/e	zwM7Oe2e1l.exe, 00000002.00000003.504433768.000001F180285000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476972337.000001F180283000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530234039.000001F180277000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504420886.000001F18027C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://fns77.ru/d	zwM7Oe2e1l.exe, 00000002.00000003.584696071.000001F180285000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584630455.000001F180277000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fns77.ru/	zwM7Oe2e1l.exe, 00000002.00000003.504283286.000001F180265000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504433768.000001F180285000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584696071.000001F180285000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000002.627384501.000001F180264000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530200851.000001F180264000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.557947549.000001F180277000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476972337.000001F180283000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.530234039.000001F180277000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.476900660.000001F180264000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.449641977.000001F180283000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584591844.000001F180264000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000002.627482009.000001F18027B000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.557786417.000001F180264000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.449602137.000001F180260000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.399547079.000001F180280000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.422978366.000001F180281000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.504420886.000001F18027C000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.584630455.000001F180277000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/l	zwM7Oe2e1l.exe, 00000002.00000002.627020793.000001F1801EB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://microsoft-ru-data.ru/r	zwM7Oe2e1l.exe, 00000002.00000003.369408265.000001F180247000.00000004.00000020.00020000.00000000.sdmp, zwM7Oe2e1l.exe, 00000002.00000003.368713421.000001F180247000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.87.218.140	fns77.ru	Russian Federation		197695	AS-REGRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679156
Start date and time: 05/08/202211:01:41	2022-08-05 11:01:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zwM7Oe2e1l (renamed file extension from none to exe)
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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.winEXE@1/0@21/2

EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:02:50	API Interceptor	37x Sleep call for process: zwM7Oe2e1l.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	5.88597431896217
TrID:	• Win64 Executable GUI Net Framework (217006/5) 47.53% • Win64 Executable GUI (202006/5) 44.25% • Win64 Executable (generic) Net Framework (21505/4) 4.71% • Win64 Executable (generic) (12005/4) 2.63% • Generic Win/DOS Executable (2004/3) 0.44%
File name:	zwM7Oe2e1l.exe
File size:	702976
MD5:	f1ab9ed37b68ace769dccaa693f162e0
SHA1:	4fc5eea47502e6ebf089910be10790614c4d4b54
SHA256:	b65bc098b475996eaabbb02bb5fee19a18c6ff2eee0062353aff696356e73b7a
SHA512:	30e0f6b070bb91443d908fb7a088629da7559f9d6a30873274b06825e861bdf122d669b16dbb707f7d0d4e7c8a7189ffef856b4a5bd6af7458b39e4e1588577e
SSDEEP:	6144:b8BIo2CR/5dEDzWfv+edsMv5kTprDd/d9mohH0gCMLM4nDp3EK4:bmInAhdEKvPXvYrR/moLS
TLSH:	5EE4F8076178EAA5F46DB1F8E5569902FA7D3C05036375EB33B2B27A1E331915F3A220
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g<S.#]=.#]=.#]=.=...!]=.76>.)]=.769.7]=.768..]=.A%9.1]=.A%>.)]=.A%8.v]=.76<.>]=.#]<..]=..$4.?]=..$.."]=..$?."]=.Rich#]=.....

File Icon

Icon Hash:	74fcd0d2d6d6d0dc

Static PE Info

General

Entrypoint:	0x140036830
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6298BBD9 [Thu Jun 2 13:32:09 2022 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:	4b5d320a7d2f87857833ae400245b4ca

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
call 00007F0C9CD4FDC4h
dec eax
add esp, 28h
jmp 00007F0C9CD4F6C7h
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax

Instruction
mov ebx, ecx
jmp 00007F0C9CD4F861h
dec eax
mov ecx, ebx
call 00007F0C9CD58FAAh
test eax, eax
je 00007F0C9CD4F865h
dec eax
mov ecx, ebx
call 00007F0C9CD59002h
dec eax
test eax, eax
je 00007F0C9CD4F839h
dec eax
add esp, 20h
pop ebx
ret
dec eax
cmp ebx, FFFFFFFFh
je 00007F0C9CD4F858h
call 00007F0C9CD50148h
int3
call 00007F0C9CD1A276h
int3
jmp 00007F0C9CD5015Ch
int3
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
lea eax, dword ptr [00029023h]
dec eax
mov ebx, ecx
dec eax
mov dword ptr [ecx], eax
test dl, 00000001h
je 00007F0C9CD4F85Ch
mov edx, 00000018h
call 00007F0C9CD4F82Bh
dec eax
mov eax, ebx
dec eax
add esp, 20h
pop ebx
ret
int3
dec eax
sub esp, 28h
call 00007F0C9CD502D8h
test eax, eax
je 00007F0C9CD4F873h
dec eax
mov eax, dword ptr [00000030h]
dec eax
mov ecx, dword ptr [eax+08h]
jmp 00007F0C9CD4F857h

Instruction
dec eax
cmp ecx, eax
je 00007F0C9CD4F866h
xor eax, eax
dec eax
cmpxchg dword ptr [00049438h], ecx
jne 00007F0C9CD4F840h
xor al, al
dec eax
add esp, 28h
ret
mov al, 01h
jmp 00007F0C9CD4F849h
int3
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
movzx eax, byte ptr [eax]

Rich Headers

Programming Language:	• [IMP] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x78acc	0x140	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x87000	0x28a49	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x82000	0x3de0	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb0000	0xa44	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6f2c0	0x70	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x6f180	0x140	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x5f000	0x778	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5d998	0x5da00	False	0.48414813501335113	data	6.384865843819584	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x5f000	0x1b47e	0x1b600	False	0.473128924086758	data	5.389641760353324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7b000	0x6978	0x4e00	False	0.30063100961538464	DOS executable (block device driver\337-\231+])	4.3547329989776475	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x82000	0x3de0	0x3e00	False	0.4913684475806452	data	5.689805709952984	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
_RDATA	0x86000	0x15c	0x200	False	0.40234375	data	3.295320723060995	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x87000	0x28a49	0x28c00	False	0.07310439033742332	data	2.947706444275165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	0xa44	0xc00	False	0.458984375	data	5.091425814699151	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x87524	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4279238655, next used block 240		
RT_ICON	0x8780c	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x87934	0x2ca8	dBase IV DBT of \300.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x8a5dc	0x1bc8	data		
RT_ICON	0x8c1a4	0x1628	dBase IV DBT of \200.DBF, blocks size 0, block length 4096, next free block index 40, next free block 353703189, next used block 353703189		
RT_ICON	0x8d7cc	0x1418	data		
RT_ICON	0x8ebe4	0xea8	data		
RT_ICON	0x8fa8c	0xba8	data		
RT_ICON	0x90634	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x90edc	0x6c8	data		
RT_ICON	0x915a4	0x608	data		
RT_ICON	0x91bac	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x92114	0xb70	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x92c84	0x94a8	data		
RT_ICON	0x9c12c	0x5488	data		
RT_ICON	0xa15b4	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 49407, next used block 4294909696		
RT_ICON	0xa57dc	0x3a48	data		
RT_ICON	0xa9224	0x25a8	data		
RT_ICON	0xab7cc	0x1a68	data		
RT_ICON	0xad234	0x10a8	data		
RT_ICON	0xae2dc	0x988	data		
RT_ICON	0xaec64	0x6b8	data		
RT_ICON	0xaf31c	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xaf784	0x148	data		
RT_MANIFEST	0xaf8cc	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	InitializeCriticalSectionEx, DecodePointer, LCMapStringEx, VerifyVersionInfoW, WriteConsoleW, ReadConsoleW, SetFilePointerEx, GetConsoleMode, GetConsoleOutputCP, FlushFileBuffers, HeapSize, HeapReAlloc, LCMapStringW, CompareStringW, SetErrorMode, EnumSystemLocalesW, GetUserDefaultLCID, WaitForMultipleObjects, CreateThread, LocalAlloc, Sleep, LocalFree, CreateMutexW, WaitForSingleObject, ReleaseMutex, CreateEventW, SetEvent, CloseHandle, ResetEvent, HeapAlloc, GetProcessHeap, ReadFile, CreatePipe, GetCurrentDirectoryA, ExitThread, CreateProcessW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, GlobalFree, QueryDosDeviceW, GetVolumeInformationW, FindFirstVolumeW, HeapFree, GetComputerNameExW, FreeEnvironmentStringsW, CreateToolhelp32Snapshot, GetLastError, Process32NextW, Process32FirstW, GetNativeSystemInfo, FindVolumeClose, GetVolumePathNamesForVolumeNameW, FindNextVolumeW, GetEnvironmentStringsW, FindFirstFileW, GetFileSizeEx, FindNextFileW, CreateFileW, GetFileAttributesW, FileTimeToSystemTime, GetFileTime, VirtualFree, WriteFile, VirtualAlloc, SetFilePointer, DeleteFileW, GetFileSize, MoveFileW, GlobalSize, LoadLibraryA, GetProcAddress, GlobalLock, FreeLibrary, GlobalUnlock, GetModuleFileNameA, VirtualAllocEx, CreateProcessA, GetComputerNameA, OpenProcess, WriteProcessMemory, CreateRemoteThread, RaiseException, SetLastError, EncodePointer, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetStdHandle, GetModuleFileNameW, GetCommandLineA, GetCommandLineW, FindClose, FindFirstFileExW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, SetEnvironmentVariableW, SetStdHandle, GetFileType, GetStringTypeW, GetLocaleInfoW, IsValidLocale
WS2_32.dll	inet_ntop
IPHLPAPI.DLL	ConvertLengthToIpv4Mask, GetAdaptersAddresses, GetAdaptersInfo
WINHTTP.dll	WinHttpSetOption, WinHttpGetIEProxyConfigForCurrentUser, WinHttpOpen, WinHttpAddRequestHeaders, WinHttpQueryHeaders, WinHttpWriteData, WinHttpQueryDataAvailable, WinHttpCloseHandle, WinHttpGetProxyForUrl, WinHttpConnect, WinHttpReadData, WinHttpReceiveResponse, WinHttpOpenRequest, WinHttpSendRequest
NETAPI32.dll	NetApiBufferFree, NetUserEnum
bcrypt.dll	BCryptCloseAlgorithmProvider, BCryptDestroyKey, BCryptDecrypt, BCryptSetProperty, BCryptGenerateSymmetricKey, BCryptOpenAlgorithmProvider, BCryptImportKeyPair, BCryptGetProperty, BCryptEncrypt
gdiplus.dll	GdipCloneImage, GdipGetImageEncoders, GdiplusStartup, GdipSaveImageToStream, GdipGetImageEncodersSize, GdipFree, GdiplusShutdown, GdipAlloc, GdipDisposeImage, GdipCreateBitmapFromHBITMAP
ntdll.dll	RtlUnwind, VerSetConditionMask, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, NtGetContextThread, NtSetContextThread, NtWriteVirtualMemory, NtResumeThread, RtlUnwindEx, RtlPcToFileHeader
mscoree.dll	CLRCreateInstance, CorBindToRuntime
USER32.dll	GetSystemMetrics, CloseWindowStation, GetDC, GetThreadDesktop, CloseDesktop, SetThreadDesktop, GetProcessWindowStation, GetDesktopWindow, OpenInputDesktop, SetProcessWindowStation, OpenWindowStationA, ReleaseDC
GDI32.dll	CreateCompatibleBitmap, SelectObject, DeleteObject, CreateCompatibleDC, DeleteDC, StretchBlt
ADVAPI32.dll	CryptAcquireContextW, CryptGenRandom, GetTokenInformation, RegQueryValueExW, GetUserNameW, ConvertSidToStringSidW, RegOpenKeyExW, RegEnumKeyExW, RegQueryInfoKeyW, RegCloseKey, LookupAccountSidW, GetSecurityInfo, OpenProcessToken, RevertToSelf, ConvertSecurityDescriptorToStringSecurityDescriptorW, ConvertStringSidToSidW
SHELL32.dll	CommandLineToArgvW
ole32.dll	CreateStreamOnHGlobal, GetHGlobalFromStream
OLEAUT32.dll	SafeArrayDestroyData, SysAllocString, SafeArrayPutElement, SysFreeString, SafeArrayCreate, SafeArrayCreateVector, SafeArrayAccessData, SafeArrayUnaccessData, SafeArrayDestroy

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8592935 32037937 08/05/22-11:02:51.521843	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	59293	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8552015 32037937 08/05/22-11:02:51.225834	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	55201	53	192.168.2.6	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.68.8.8.8565505 32037937 08/05/22-11:02:54.471667	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	56550	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8565915 32037937 08/05/22-11:02:52.438751	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	56591	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8557885 32037938 08/05/22-11:04:47.473277	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	55788	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8611165 32037937 08/05/22-11:02:53.326830	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	61116	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8587235 32037937 08/05/22-11:02:51.809410	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	58723	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8631045 32037938 08/05/22-11:04:09.074489	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	63104	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8586895 32037938 08/05/22-11:03:44.188103	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	58689	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8616075 32037937 08/05/22-11:02:54.097826	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	61607	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8540155 32037938 08/05/22-11:03:31.447464	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	54015	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8653675 32037938 08/05/22-11:04:21.925023	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	65367	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8603505 32037937 08/05/22-11:02:52.686111	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	60350	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8517485 32037937 08/05/22-11:02:52.976163	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	51748	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8598715 32037938 08/05/22-11:03:07.881163	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	59871	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8519715 32037937 08/05/22-11:02:52.201354	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	51971	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8511945 32037938 08/05/22-11:03:18.845501	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	51194	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8576695 32037938 08/05/22-11:04:34.382443	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	57669	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8509585 32037937 08/05/22-11:02:53.714812	UDP	2037937	ET TROJAN Woody RAT CnC Domain (microsoft-ru-data .ru) in DNS Lookup	50958	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8528585 32037938 08/05/22-11:02:54.797599	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	52858	53	192.168.2.6	8.8.8.8
192.168.2.68.8.8.8530495 32037938 08/05/22-11:03:56.868334	UDP	2037938	ET TROJAN Woody RAT CnC Domain (fns77 .ru) in DNS Lookup	53049	53	192.168.2.6	8.8.8.8

Network Port Distribution

Total Packets: 72

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:02:54.932476997 CEST	49763	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:54.932529926 CEST	443	49763	194.87.218.140	192.168.2.6
Aug 5, 2022 11:02:54.932723045 CEST	49763	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:54.938019037 CEST	49763	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:54.938045979 CEST	443	49763	194.87.218.140	192.168.2.6
Aug 5, 2022 11:02:56.702358007 CEST	443	49763	194.87.218.140	192.168.2.6
Aug 5, 2022 11:02:56.703921080 CEST	49764	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:56.703977108 CEST	443	49764	194.87.218.140	192.168.2.6
Aug 5, 2022 11:02:56.704104900 CEST	49764	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:56.704849958 CEST	49764	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:56.704869986 CEST	443	49764	194.87.218.140	192.168.2.6
Aug 5, 2022 11:02:59.874269009 CEST	443	49764	194.87.218.140	192.168.2.6
Aug 5, 2022 11:02:59.889511108 CEST	49765	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:59.889550924 CEST	443	49765	194.87.218.140	192.168.2.6
Aug 5, 2022 11:02:59.889677048 CEST	49765	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:59.890806913 CEST	49765	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:02:59.890829086 CEST	443	49765	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:03.038507938 CEST	443	49765	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:03.058084965 CEST	49766	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:03.058160067 CEST	443	49766	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:03.058295012 CEST	49766	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:03.058861971 CEST	49766	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:03.058887005 CEST	443	49766	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:06.206222057 CEST	443	49766	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:07.906095028 CEST	49768	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:07.906147003 CEST	443	49768	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:07.906265020 CEST	49768	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:07.908401012 CEST	49768	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:07.908430099 CEST	443	49768	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:09.278125048 CEST	443	49768	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:09.279557943 CEST	49769	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:09.279584885 CEST	443	49769	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:09.279737949 CEST	49769	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:09.280375004 CEST	49769	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:09.280385017 CEST	443	49769	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:12.414793015 CEST	443	49769	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:12.431951046 CEST	49770	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:12.432001114 CEST	443	49770	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:12.432136059 CEST	49770	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:12.432653904 CEST	49770	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:12.432673931 CEST	443	49770	194.87.218.140	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:03:15.486304998 CEST	443	49770	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:15.492050886 CEST	49771	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:15.492100000 CEST	443	49771	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:15.492202044 CEST	49771	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:15.492857933 CEST	49771	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:15.492883921 CEST	443	49771	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:18.626404047 CEST	443	49771	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:18.924467087 CEST	49772	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:18.924510956 CEST	443	49772	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:18.924639940 CEST	49772	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:18.925410032 CEST	49772	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:18.925437927 CEST	443	49772	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:21.694861889 CEST	443	49772	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:21.696540117 CEST	49773	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:21.696593046 CEST	443	49773	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:21.696805000 CEST	49773	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:21.697556019 CEST	49773	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:21.697581053 CEST	443	49773	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:24.862427950 CEST	443	49773	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:24.879900932 CEST	49774	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:24.879965067 CEST	443	49774	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:24.880069017 CEST	49774	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:24.880968094 CEST	49774	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:24.880989075 CEST	443	49774	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:28.030345917 CEST	443	49774	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:28.032383919 CEST	49785	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:28.032428980 CEST	443	49785	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:28.032536030 CEST	49785	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:28.033236980 CEST	49785	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:28.033261061 CEST	443	49785	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:31.102269888 CEST	443	49785	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:31.623568058 CEST	49788	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:31.623613119 CEST	443	49788	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:31.623712063 CEST	49788	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:31.624454021 CEST	49788	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:31.624475956 CEST	443	49788	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:34.238286972 CEST	443	49788	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:34.240503073 CEST	49791	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:34.240567923 CEST	443	49791	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:34.240694046 CEST	49791	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:34.241524935 CEST	49791	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:34.241550922 CEST	443	49791	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:37.406433105 CEST	443	49791	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:37.408396959 CEST	49796	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:37.408461094 CEST	443	49796	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:37.408571005 CEST	49796	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:37.410048962 CEST	49796	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:37.410079956 CEST	443	49796	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:40.578552961 CEST	443	49796	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:40.579910994 CEST	49797	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:40.579965115 CEST	443	49797	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:40.580050945 CEST	49797	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:40.580753088 CEST	49797	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:40.580779076 CEST	443	49797	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:43.755327940 CEST	443	49797	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:44.207053900 CEST	49799	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:44.207096100 CEST	443	49799	194.87.218.140	192.168.2.6
Aug 5, 2022 11:03:44.207191944 CEST	49799	443	192.168.2.6	194.87.218.140
Aug 5, 2022 11:03:44.207844973 CEST	49799	443	192.168.2.6	194.87.218.140

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:02:51.225833893 CEST	55201	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:51.242561102 CEST	53	55201	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:51.521842957 CEST	59293	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:51.541172028 CEST	53	59293	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:51.809410095 CEST	58723	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:51.828824997 CEST	53	58723	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:52.201354027 CEST	51971	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:52.220902920 CEST	53	51971	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:52.438750982 CEST	56591	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:52.457427025 CEST	53	56591	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:52.686110973 CEST	60350	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:52.705450058 CEST	53	60350	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:52.976162910 CEST	51748	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:52.995296001 CEST	53	51748	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:53.326829910 CEST	61116	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:53.343807936 CEST	53	61116	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:53.714812040 CEST	50958	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:53.735369921 CEST	53	50958	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:54.097826004 CEST	61607	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:54.117041111 CEST	53	61607	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:54.471667051 CEST	56550	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:54.490464926 CEST	53	56550	8.8.8.8	192.168.2.6
Aug 5, 2022 11:02:54.797599077 CEST	52858	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:02:54.908832073 CEST	53	52858	8.8.8.8	192.168.2.6
Aug 5, 2022 11:03:07.881162882 CEST	59871	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:03:07.902704954 CEST	53	59871	8.8.8.8	192.168.2.6
Aug 5, 2022 11:03:18.845500946 CEST	51194	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:03:18.922394037 CEST	53	51194	8.8.8.8	192.168.2.6
Aug 5, 2022 11:03:31.447463989 CEST	54015	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:03:31.524036884 CEST	53	54015	8.8.8.8	192.168.2.6
Aug 5, 2022 11:03:44.188102961 CEST	58689	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:03:44.205487967 CEST	53	58689	8.8.8.8	192.168.2.6
Aug 5, 2022 11:03:56.868334055 CEST	53049	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:03:56.983062983 CEST	53	53049	8.8.8.8	192.168.2.6
Aug 5, 2022 11:04:09.074489117 CEST	63104	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:04:09.183706999 CEST	53	63104	8.8.8.8	192.168.2.6
Aug 5, 2022 11:04:21.925023079 CEST	65367	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:04:21.943284988 CEST	53	65367	8.8.8.8	192.168.2.6
Aug 5, 2022 11:04:34.382442951 CEST	57669	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:04:34.402014971 CEST	53	57669	8.8.8.8	192.168.2.6
Aug 5, 2022 11:04:47.473277092 CEST	55788	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:04:47.492806911 CEST	53	55788	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 11:02:51.225833893 CEST	192.168.2.6	8.8.8.8	0x5295	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:51.521842957 CEST	192.168.2.6	8.8.8.8	0xa085	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:51.809410095 CEST	192.168.2.6	8.8.8.8	0x4f9b	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:52.201354027 CEST	192.168.2.6	8.8.8.8	0xb567	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:52.438750982 CEST	192.168.2.6	8.8.8.8	0x22cd	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:52.686110973 CEST	192.168.2.6	8.8.8.8	0xe5fe	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:52.976162910 CEST	192.168.2.6	8.8.8.8	0x558a	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 11:02:53.326829910 CEST	192.168.2.6	8.8.8.8	0xb947	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:53.714812040 CEST	192.168.2.6	8.8.8.8	0x2a54	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:54.097826004 CEST	192.168.2.6	8.8.8.8	0xf592	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:54.471667051 CEST	192.168.2.6	8.8.8.8	0x8e86	Standard query (0)	microsoft-ru-data.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:02:54.797599077 CEST	192.168.2.6	8.8.8.8	0x4036	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:07.881162882 CEST	192.168.2.6	8.8.8.8	0xc1ee	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:18.845500946 CEST	192.168.2.6	8.8.8.8	0xa886	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:31.447463989 CEST	192.168.2.6	8.8.8.8	0xbfa	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:44.188102961 CEST	192.168.2.6	8.8.8.8	0xfae4	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:56.868334055 CEST	192.168.2.6	8.8.8.8	0x3df8	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:04:09.074489117 CEST	192.168.2.6	8.8.8.8	0xd6df	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:04:21.925023079 CEST	192.168.2.6	8.8.8.8	0x730d	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:04:34.382442951 CEST	192.168.2.6	8.8.8.8	0xe5e4	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 11:04:47.473277092 CEST	192.168.2.6	8.8.8.8	0x46a8	Standard query (0)	fns77.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 11:02:54.908832073 CEST	8.8.8.8	192.168.2.6	0x4036	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:07.902704954 CEST	8.8.8.8	192.168.2.6	0xc1ee	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:18.922394037 CEST	8.8.8.8	192.168.2.6	0xa886	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:31.524036884 CEST	8.8.8.8	192.168.2.6	0xbfa	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:44.205487967 CEST	8.8.8.8	192.168.2.6	0xfae4	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:03:56.983062983 CEST	8.8.8.8	192.168.2.6	0x3df8	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:04:09.183706999 CEST	8.8.8.8	192.168.2.6	0xd6df	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:04:21.943284988 CEST	8.8.8.8	192.168.2.6	0x730d	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:04:34.402014971 CEST	8.8.8.8	192.168.2.6	0xe5e4	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)
Aug 5, 2022 11:04:47.492806911 CEST	8.8.8.8	192.168.2.6	0x46a8	No error (0)	fns77.ru		194.87.218.140	A (IP address)	IN (0x0001)

Statistics

No statistics

System Behavior

Analysis Process: zwM7Oe2e1l.exe PID: 1316, Parent PID: 3560

General

Target ID:	2

Start time:	11:02:49
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\zwM7Oe2e1l.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\zwM7Oe2e1l.exe"
Imagebase:	0x7ff7c3f90000
File size:	702976 bytes
MD5 hash:	F1AB9ED37B68ACE769DCCAA693F162E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly