
**ID:** 827054
**Sample Name:** server.exe
**Cookbook:** default.jbs
**Time:** 14:38:10
**Date:** 15/03/2023
**Version:** 37.0.0 Beryl

# Table of Contents


Table of Contents 2
Windows Analysis Report server.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Compliance 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
System Summary 6
Data Obfuscation 6
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
Anti Debugging 6
Stealing of Sensitive Information 6
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Rich Headers 15
Data Directories 15
Sections 15
Resources 15
Imports 17
Possible Origin 17
Network Behavior 17
Snort IDS Alerts 17
Network Port Distribution 18
TCP Packets 18
UDP Packets 18

DNS Queries 18
DNS Answers 18
HTTP Request Dependency Graph 18
Statistics 19
System Behavior 19
Analysis Process: server.exePID: 3536, Parent PID: 3528 19
General 19
File Activities 20
Disassembly 20

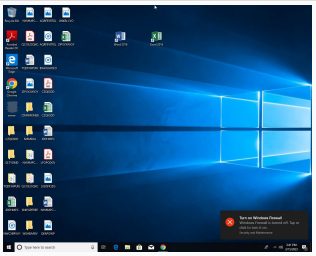
# Windows Analysis Report

## server.exe

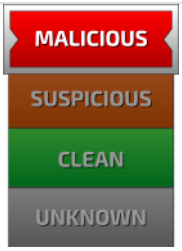
## Overview

### General Information

| | |
|---|---|
| Sample Name: | server.exe |
| Analysis ID: | 827054 |
| MD5: | 768928d17e8d… |
| SHA1: | 8ce488487dc1… |
| SHA256: | 5d0be9aaad98… |
| Tags: | agenziaentrate exe gozi isfb ITA mef mise ursnif |
| Infos: | |



### Detection



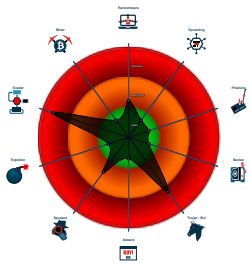

Ursnif

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

### Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected Ursnif
- Detected unpacking (changes PE se…
- Snort IDS alert for network traffic
- Writes or reads registry keys via WMI
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Found evasive API chain (may stop…
- Writes registry values via WMI
- Uses 32bit PE files

### Classification



## Process Tree

- **System is w10x64**
- server.exe (PID: 3536 cmdline: C:\Users\user\Desktop\server.exe MD5: 768928D17E8D3489407B540DBAD4A770)
- **cleanup**

## Malware Threat Intel

Provided by malpedia

| Name | Description | Attribution | Blogpost URLs | Link |
|---|---|---|---|---|
| **Gozi, Ursnif** | 2000 Ursnif aka Snifula2006 Gozi v1.0, Gozi CRM, CRM, Papras2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)-> 2010 Gozi Prinimalka -> Vawtrak/NeverquestIn 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed.It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module. | No Attribution | **http://** blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.htmlhttp://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html | **http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi |

## Malware Configuration

**Threatname: Ursnif**

```
{
  "RSA Public Key":
"ScCitKVnthsrIejolA7zuBWvwII2di/DH3GlyTtkQAl5+NYn11P8hoApgIAx8QgiEaRicK3ETZq3j2ua44XjJevEH0XzzTqZAT3wkYswDxrBkgZMCwo6YXkhXitvoh3eARDtRDEkQsoLHZ9GnSskgPPZhcXZcW5DEVGUxmtbXgDaTXEE
ASp94TxsSTq8LcHFcoUD/3qCUIKISKD7sIV0hgpJQ8kx5Fr/zREoX54YDyuxKi/xJ3SBIavWF9UPU+YwvxpBDYMFrMsKJrjGUlpoQZehisJjttb1cTtggelEGnFr5O2GXefQUuwrSizDeVnMRSAHdds+AiqlPxEl1nFzSfnHhHtw7Ql8J
tPTws7Z1Ho=",
  "c2_domain": [
    "checklist.skype.com",
    "5.44.43.17",
    "31.41.44.108",
    "62.173.138.213",
    "109.248.11.174"
  ],
  "botnet": "7714",
  "server": "50",
  "serpent_key": "lk8hY4nisKQzZKXE",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


# Yara Signatures

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.568856386.0000000002E48000.00000040.00000020.00020000.00000000.sdmp | Windows_Trojan_RedLineStealer_ed346e4c | unknown | unknown | • 0x6b65:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B |
| 00000000.00000003.459546153.0000000005258000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000000.00000003.459546153.0000000005258000.00000004.00000020.00020000.00000000.sdmp | Windows_Trojan_Gozi_fd494041 | unknown | unknown | • 0x1228:$a1: /C ping localhost -n %u && del "%s"<br>• 0xea8:$a2: /C "copy "%s" "%s" /y && "%s" "%s"<br>• 0xf00:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S"<br>• 0xa9c:$a5: filename="%.4u.%lu"<br>• 0x63a:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s<br>• 0x876:$a8: %08X-%04X-%04X-%04X-%08X%04X<br>• 0xbb7:$a8: %08X-%04X-%04X-%04X-%08X%04X<br>• 0xe6d:$a9: &whoami=%s<br>• 0xe56:$a10: %u.%u_%u_%u_x%u<br>• 0xd63:$a11: size=%u&hash=0x%08x<br>• 0xb1d:$a12: &uptime=%u<br>• 0x6fb:$a13: %systemroot%\system32\c_1252.nls<br>• 0x1298:$a14: IE10RunOnceLastShown_TIMESTAMP |
| 00000000.00000003.459546153.0000000005258000.00000004.00000020.00020000.00000000.sdmp | Windows_Trojan_Gozi_261f5ac5 | unknown | unknown | • 0xb54:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x<br>• 0x63a:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s<br>• 0xa68:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu"<br>• 0xcf2:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s)<br>• 0xd96:$a9: Software\AppDataLow\Software\Microsoft\<br>• 0x1ca0:$a9: Software\AppDataLow\Software\Microsoft\ |
| 00000000.00000002.568965498.0000000005258000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |

Click to see the 27 entries

# Sigma Signatures

**No Sigma rule has matched**

# Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 5.44.43.17

| | |
|---|---|
| Timestamp: | 192.168.2.45.44.43.1749695802033203 03/15/23-14:40:37.858863 |
| SID: | 2033203 |
| Source Port: | 49695 |

| | |
|---|---|
| Destination Port: | 80 |
| Protocol: | TCP |
| Classtype: | A Network Trojan was detected |

## Joe Sandbox Signatures

### AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

### Compliance

Detected unpacking (overwrites its own PE header)

### Networking

Snort IDS alert for network traffic

### Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

### E-Banking Fraud

Yara detected Ursnif

### System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

### Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

### Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

### Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking system information)

### Anti Debugging

Found API chain indicative of debugger detection

### Stealing of Sensitive Information

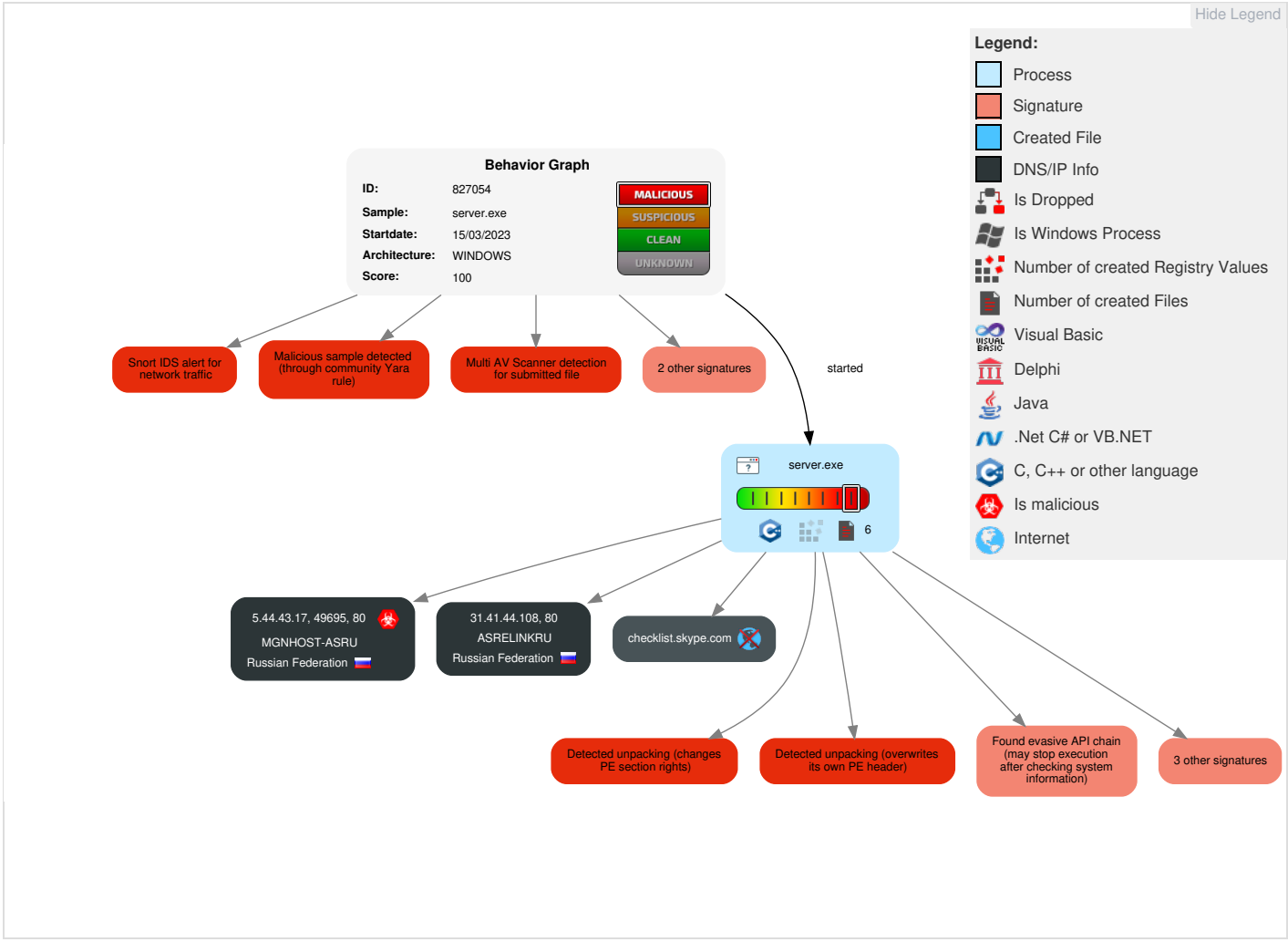
Yara detected Ursnif

Yara detected Ursnif

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | 2 Windows Management Instrumentation | Path Interception | Path Interception | 1 1 Virtualization/Sandbox Evasion | 1 Input Capture | 1 System Time Discovery | Remote Services | 1 Input Capture | Exfiltration Over Other Network Medium | 2 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | 1 Data Encrypted for Impact |
| Default Accounts | 1 2 Native API | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 1 Obfuscated Files or Information | LSASS Memory | 1 1 Security Software Discovery | Remote Desktop Protocol | 1 1 Archive Collected Data | Exfiltration Over Bluetooth | 1 Ingress Tool Transfer | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | 2 1 Software Packing | Security Account Manager | 1 1 Virtualization/Sandbox Evasion | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 2 Non-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 Process Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | 1 2 Application Layer Protocol | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Software Packing | LSA Secrets | 1 Account Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Steganography | Cached Domain Credentials | 1 System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | Abuse Accessibility Features |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Compile After Delivery | DCSync | 1 Remote System Discovery | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points | | Data Encrypted for Impact |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Indicator Removal from Tools | Proc Filesystem | 1 2 4 System Information Discovery | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade to Insecure Protocols | | Generate Fraudulent Advertising Revenue |

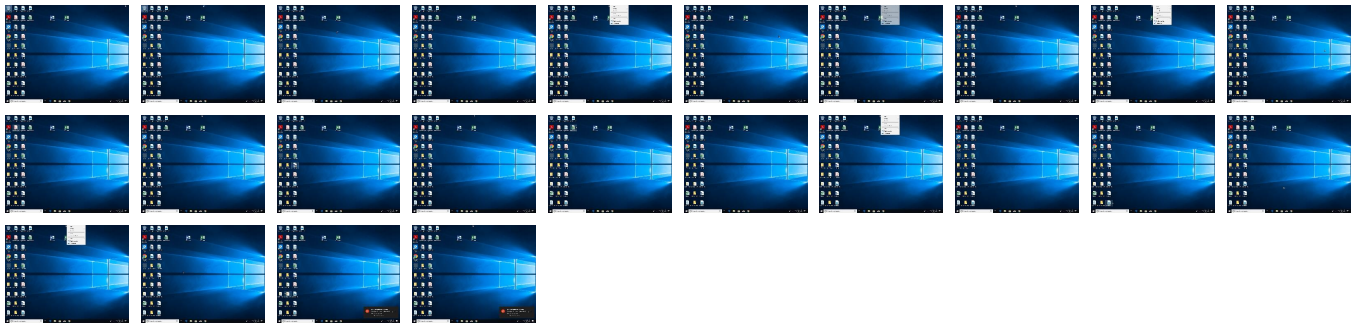
## Behavior Graph




## 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 |
|---|---|---|---|---|
| server.exe | 55% | Virustotal | | Browse |
| server.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.2.server.exe.2ce0000.2.unpack | 100% | Avira | HEUR/AGEN.1245293 | | Download File |
| 0.2.server.exe.400000.0.unpack | 100% | Avira | TR/Crypt.XPACK.Gen7 | | Download File |

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://5.44.43.17/drew/4g9Pq9f8yl_2BqLNg_2F/GsF66vmh2Tpicwg37xs/IeFtLuJ4Vgq9WwijsD2n0d/Bquuj0kLXj_2B | 0% | Avira URL Cloud | safe | |
| http://5.44.43.17/ | 0% | Avira URL Cloud | safe | |
| http://31.41.44.108/drew/FJTU0wze8Hjvm_2BHka/T78K158O_2Fv5farATygbE/7uQJsjJeUPlO2/LBUhKSJa/o4FD53ecF | 0% | Avira URL Cloud | safe | |
| http://5.44.43.17/98D0-4585-A1ED-B2838757AE1B | 0% | Avira URL Cloud | safe | |
| http://5.44.43.17/-A1ED-B2838757AE1B | 0% | Avira URL Cloud | safe | |
| http://5.44.43.17/drew/4g9Pq9f8yl_2BqLNg_2F/GsF66vmh2Tpicwg37xs/IeFtLuJ4Vgq9WwijsD2n0d/Bquuj0kLXj_2B/g9_2Bh6q/18_2Bd4Y19mjSIvebXNvx4u/IKPQjubsH_/2BffqZNZA6lqyycQo/1wN43eb54EKC/UkUZJXRrn4j/R3115Fw4Czb8SK/xar7XimyyrkEE9m9c0UP0/1KSNpQlordpxo1Ws/_2B6QH8tLTSTNrP/6dO_2BuUeu5EmaGfZI/wcja66YPQ/Z_2B4nfOuMl7_2BnQaBq/8KUwwwam.jlk | 0% | Avira URL Cloud | safe | |
| http://31.41.44.108/32 | 0% | Avira URL Cloud | safe | |
| http://5.44.43.17/ | 1% | Virustotal | | Browse |
| http://31.41.44.108/ | 0% | Avira URL Cloud | safe | |
| http://31.41. | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| checklist.skype.com | unknown | unknown | false | | high |

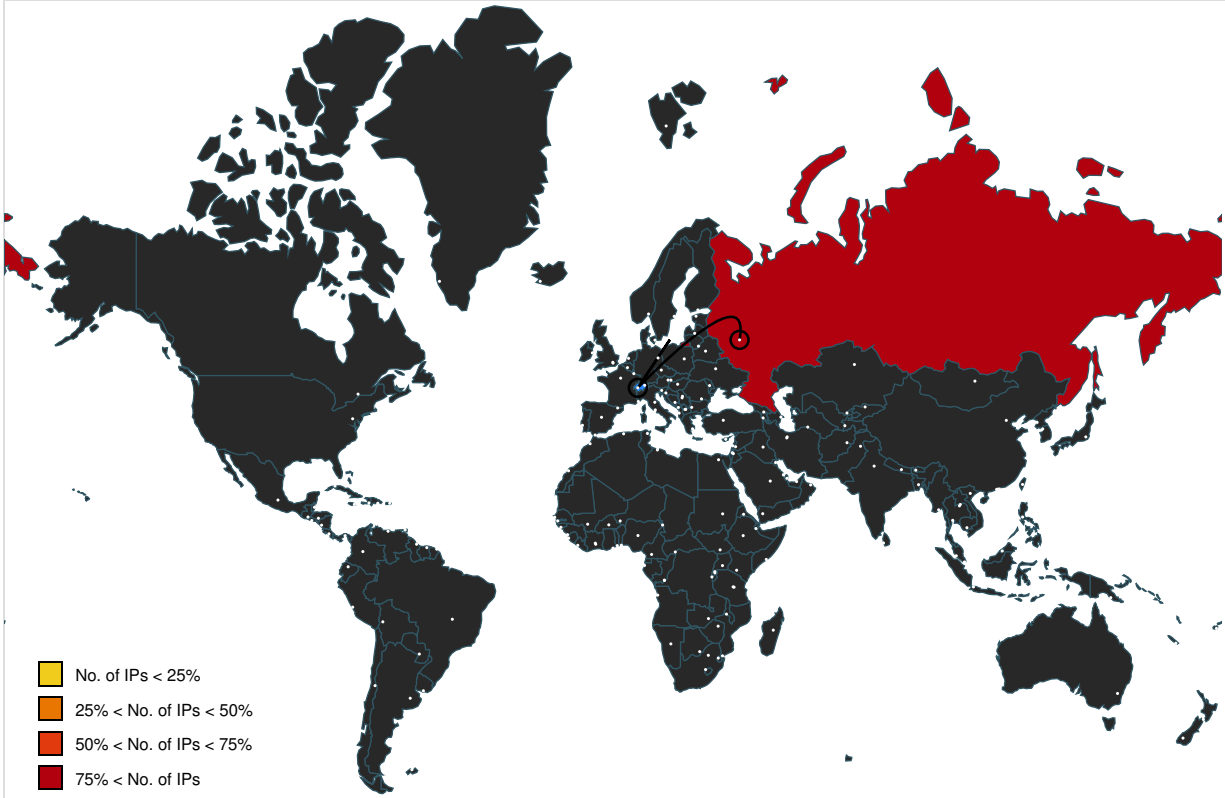
## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://5.44.43.17/drew/4g9Pq9f8yl_2BqLNg_2F/GsF66vmh2Tpicwg37xs/IeFtLuJ4Vgq9WwijsD2n0d/Bquuj0kLXj_2B/g9_2Bh6q/18_2Bd4Y19mjSIvebXNvx4u/IKPQjubsH_/2BffqZNZA6lqyycQo/1wN43eb54EKC/UkUZJXRrn4j/R3115Fw4Czb8SK/xar7XimyyrkEE9m9c0UP0/1KSNpQlordpxo1Ws/_2B6QH8tLTSTNrP/6dO_2BuUeu5EmaGfZI/wcja66YPQ/Z_2B4nfOuMl7_2BnQaBq/8KUwwwam.jlk | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://5.44.43.17/drew/4g9Pq9f8yl_2BqLNg_2F/GsF66vmh2Tpicwg37xs/IeFtLuJ4Vgq9WwijsD2n0d/Bquuj0kLXj_2B | server.exe, 00000000.00000002.568866270.0000000002EB8000.00000004.00000020.00020000.00000000.sdmp, server.exe, 00000000.00000002.568866270.0000000002EAC000.00000004.00000020.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://5.44.43.17/ | server.exe, 00000000.00000002.568866270.0000000002E5E000.00000004.00000020.00020000.00000000.sdmp | false | • 1%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |
| http://5.44.43.17/-A1ED-B2838757AE1B | server.exe, 00000000.00000002.568866270.0000000002E5E000.00000004.00000020.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://31.41.44.108/drew/FJTU0wze8Hjvm_2BHka/T78K158O_2Fv5farATygbE/7uQJsjJeUPlO2/LBUhKSJa/o4FD53ecF | server.exe, 00000000.00000002.568866270.0000000002E5E000.00000004.00000020.00020000.00000000.sdmp, server.exe, 00000000.00000002.568866270.0000000002EAC000.00000004.00000020.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://5.44.43.17/98D0-4585-A1ED-B2838757AE1B | server.exe, 00000000.00000002.568866270.0000000002E5E000.00000004.00000020.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://31.41.44.108/ | server.exe, 00000000.00000002.568866270.0000000002E5E000.00000004.00000020.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://31.41.44.108/32 | server.exe, 00000000.00000002.568866270.0000000002E5E000.00000004.00000020.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://31.41. | server.exe, 00000000.00000002.568929049.00000000049BC000.00000004.00000010.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | low |
| http://checklist.skype.com/drew/RCiQyn59/Gow2vU3BObfVI7A8uLXOgnm/720Rvxrh27/9sCisgCQ1dbhwi3H4/XmYN2I | server.exe, 00000000.00000002.568866270.0000000002EAC000.00000004.00000020.00020000.00000000.sdmp | false | | high |

## World Map of Contacted IPs




### Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 5.44.43.17 | unknown | Russian Federation | | 202423 | MGNHOST-ASRU | true |
| 31.41.44.108 | unknown | Russian Federation | | 56577 | ASRELINKRU | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 37.0.0 Beryl |
| Analysis ID: | 827054 |
| Start date and time: | 2023-03-15 14:38:10 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 12s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 7 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Sample file name: | server.exe |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@1/0@1/2 |
| EGA Information: | • Successful, ratio: 100% |

| | |
|---|---|
| HDC Information: | • Successful, ratio: 56.7% (good quality ratio 55.1%)<br>• Quality average: 82%<br>• Quality standard deviation: 26.5% |
| HCA Information: | • Successful, ratio: 95%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .exe |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

## Simulations

### Behavior and APIs

No simulations

## 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) Intel 80386, for MS Windows |
| Entropy (8bit): | 6.191671893434653 |

| | |
|---|---|
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | server.exe |
| File size: | 316928 |
| MD5: | 768928d17e8d3489407b540dbad4a770 |
| SHA1: | 8ce488487dc133ef92dec536608b0c1056a3e16a |
| SHA256: | 5d0be9aaad980137d68677d7ef3758d9ce7a4e2d170df0abee803f64b14dcd67 |
| SHA512: | 0827c24c00d00ce10e5f6732d29efed6a051eafcc9aeb6a7c69d5b89615f7eb49b5333b6d5614613b0e64f792b3ff6d850108eb736eb1169eccbda09be3ac869 |
| SSDEEP: | 3072:3SVRi5/ELPnpP0SbcTS7ipobb2m+9vAh2QlNlfkkVjJ:Cri5ELBcV3qbAln5NJ |
| TLSH: | CC642A1393E1BD85E96A8B729E1ED6F8761EF690CE0D776922289F1F04B1076C263710 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:..@[..@[..@[..^.>.`[..^./.T[..^.9.#<br>[..g...I[..@[..3[..^.0.A[..^...A[..^.+.A[..Rich@[.....PE..L.....^b..... |

## File Icon

| | |
|---|---|
| Icon Hash: | a4a4a08484b4a4e0 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x404f66 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | EXECUTABLE_IMAGE, 32BIT_MACHINE |
| DLL Characteristics: | TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x625E87B1 [Tue Apr 19 09:58:09 2022 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 5 |
| OS Version Minor: | 0 |
| File Version Major: | 5 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 5 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 25b97b20ea5f74ae1a1939bb76680477 |

### Entrypoint Preview

| Instruction |
|---|
| call 00007FBBDCB55A6Bh |
| jmp 00007FBBDCB5393Eh |
| mov edi, edi |
| push ecx |
| mov dword ptr [ecx], 0040125Ch |
| call 00007FBBDCB55AEEh |
| pop ecx |
| ret |
| mov edi, edi |
| push ebp |
| mov ebp, esp |
| push esi |
| mov esi, ecx |
| call 00007FBBDCB53AA8h |
| test byte ptr [ebp+08h], 00000001h |
| je 00007FBBDCB53AC9h |
| push esi |

| Instruction |
| --- |
| call 00007FBBDCB53D75h |
| pop ecx |
| mov eax, esi |
| pop esi |
| pop ebp |
| retn 0004h |
| mov edi, edi |
| push ebp |
| mov ebp, esp |
| mov ecx, dword ptr [ebp+08h] |
| push ebx |
| xor ebx, ebx |
| push esi |
| push edi |
| cmp ecx, ebx |
| je 00007FBBDCB53AC9h |
| mov edi, dword ptr [ebp+0Ch] |
| cmp edi, ebx |
| jnbe 00007FBBDCB53ADDh |
| call 00007FBBDCB55D4Eh |
| push 00000016h |
| pop esi |
| mov dword ptr [eax], esi |
| push ebx |
| push ebx |
| push ebx |
| push ebx |
| push ebx |
| call 00007FBBDCB55CD7h |
| add esp, 14h |
| mov eax, esi |
| jmp 00007FBBDCB53AF2h |
| mov esi, dword ptr [ebp+10h] |
| cmp esi, ebx |
| jne 00007FBBDCB53AC6h |
| mov byte ptr [ecx], bl |
| jmp 00007FBBDCB53A9Ch |
| mov edx, ecx |
| mov al, byte ptr [esi] |
| mov byte ptr [edx], al |
| inc edx |
| inc esi |
| cmp al, bl |
| je 00007FBBDCB53AC5h |
| dec edi |
| jne 00007FBBDCB53AB5h |
| cmp edi, ebx |
| jne 00007FBBDCB53AD2h |
| mov byte ptr [ecx], bl |
| call 00007FBBDCB55D13h |
| push 00000022h |
| pop ecx |
| mov dword ptr [eax], ecx |
| mov esi, ecx |
| jmp 00007FBBDCB53A83h |
| xor eax, eax |
| pop edi |
| pop esi |
| pop ebx |

| Instruction |
|---|
| pop ebp |
| ret |
| push 0000000Ch |
| push 0040EEC0h |
| call 00007FBBDCB54DF4h |
| and dword ptr [ebp-1Ch], 00000000h |
| mov esi, dword ptr [ebp+08h] |
| cmp esi, dword ptr [02AE8870h] |
| jnbe 00007FBBDCB53AE4h |
| push 00000004h |
| call 00007FBBDCB55E70h |
| pop ecx |
| and dword ptr [ebp+00h], 00000000h |

## Rich Headers

| | |
|---|---|
| Programming Language: | • [C++] VS2008 build 21022<br>• [ASM] VS2008 build 21022<br>• [ C ] VS2008 build 21022<br>• [IMP] VS2005 build 50727<br>• [RES] VS2008 build 21022<br>• [LNK] VS2008 build 21022 |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0xf14c | 0x64 | .text |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x26e9000 | 0x1f6e8 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x2709000 | 0xa40 | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x11c0 | 0x1c | .text |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x2d98 | 0x40 | .text |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x1000 | 0x184 | .text |
| 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 | 0xea34 | 0xec00 | False | 0.5837526483050848 | data | 6.736125354250025 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .data | 0x10000 | 0x26d89c8 | 0x17400 | unknown | unknown | unknown | unknown | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .rsrc | 0x26e9000 | 0x1f6e8 | 0x1f800 | False | 0.4157831101190476 | data | 4.733170034701941 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x2709000 | 0x78fc | 0x7a00 | False | 0.0759157274590164 | data | 0.9356665533967813 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

## Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| AFX_DIALOG_LAYOUT | 0x2704e08 | 0x2 | data | | |
| AFX_DIALOG_LAYOUT | 0x2704df0 | 0xe | data | | |
| AFX_DIALOG_LAYOUT | 0x2704e00 | 0x2 | data | | |

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| JOSEFUZITILEP | 0x27034a8 | 0x18d4 | ASCII text, with very long lines (6356), with no line terminators | Serbian | Italy |
| MOXUCAKOSAMIZIJAYIG | 0x2702cd0 | 0x7d1 | ASCII text, with very long lines (2001), with no line terminators | Serbian | Italy |
| RT_CURSOR | 0x2704e10 | 0x330 | Device independent bitmap graphic, 48 x 96 x 1, image size 0 | | |
| RT_CURSOR | 0x2705140 | 0x130 | Device independent bitmap graphic, 32 x 64 x 1, image size 0 | | |
| RT_CURSOR | 0x2705298 | 0xea8 | Device independent bitmap graphic, 48 x 96 x 8, image size 0 | | |
| RT_CURSOR | 0x2706140 | 0x8a8 | Device independent bitmap graphic, 32 x 64 x 8, image size 0 | | |
| RT_CURSOR | 0x27069e8 | 0x568 | Device independent bitmap graphic, 16 x 32 x 8, image size 0 | | |
| RT_CURSOR | 0x2706f80 | 0x130 | Device independent bitmap graphic, 32 x 64 x 1, image size 0 | | |
| RT_CURSOR | 0x27070b0 | 0xb0 | Device independent bitmap graphic, 16 x 32 x 1, image size 0 | | |
| RT_ICON | 0x26e9c60 | 0xea8 | Device independent bitmap graphic, 48 x 96 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26eab08 | 0x8a8 | Device independent bitmap graphic, 32 x 64 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26eb3b0 | 0x6c8 | Device independent bitmap graphic, 24 x 48 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26eba78 | 0x568 | Device independent bitmap graphic, 16 x 32 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26ebfe0 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x26ee588 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x26ef630 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x26efb00 | 0xea8 | Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors | Serbian | Italy |
| RT_ICON | 0x26f09a8 | 0x8a8 | Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors | Serbian | Italy |
| RT_ICON | 0x26f1250 | 0x6c8 | Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors | Serbian | Italy |
| RT_ICON | 0x26f1918 | 0x568 | Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors | Serbian | Italy |
| RT_ICON | 0x26f1e80 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 9216 | Serbian | Italy |
| RT_ICON | 0x26f4428 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4096 | Serbian | Italy |
| RT_ICON | 0x26f54d0 | 0x988 | Device independent bitmap graphic, 24 x 48 x 32, image size 2304 | Serbian | Italy |
| RT_ICON | 0x26f5e58 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 1024 | Serbian | Italy |
| RT_ICON | 0x26f6338 | 0xea8 | Device independent bitmap graphic, 48 x 96 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26f71e0 | 0x8a8 | Device independent bitmap graphic, 32 x 64 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26f7a88 | 0x568 | Device independent bitmap graphic, 16 x 32 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26f7ff0 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x26fa598 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x26fb640 | 0x988 | Device independent bitmap graphic, 24 x 48 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x26fbfc8 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x26fc498 | 0xea8 | Device independent bitmap graphic, 48 x 96 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26fd340 | 0x8a8 | Device independent bitmap graphic, 32 x 64 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26fdbe8 | 0x6c8 | Device independent bitmap graphic, 24 x 48 x 8, image size 0 | Serbian | Italy |
| RT_ICON | 0x26fe2b0 | 0x568 | Device independent bitmap graphic, 16 x 32 x 8, image size 0 | Serbian | Italy |

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0x26fe818 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x2700dc0 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x2701e68 | 0x988 | Device independent bitmap graphic, 24 x 48 x 32, image size 0 | Serbian | Italy |
| RT_ICON | 0x27027f0 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 0 | Serbian | Italy |
| RT_STRING | 0x2707380 | 0x2be | data | | |
| RT_STRING | 0x2707640 | 0x492 | data | | |
| RT_STRING | 0x2707ad8 | 0x5c6 | data | | |
| RT_STRING | 0x27080a0 | 0x118 | data | | |
| RT_STRING | 0x27081b8 | 0x52a | data | | |
| RT_ACCELERATOR | 0x2704d80 | 0x48 | data | Serbian | Italy |
| RT_ACCELERATOR | 0x2704dc8 | 0x18 | data | Serbian | Italy |
| RT_GROUP_CURSOR | 0x2705270 | 0x22 | data | | |
| RT_GROUP_CURSOR | 0x2706f50 | 0x30 | data | | |
| RT_GROUP_CURSOR | 0x2707160 | 0x22 | data | | |
| RT_GROUP_ICON | 0x26fc430 | 0x68 | data | Serbian | Italy |
| RT_GROUP_ICON | 0x26efa98 | 0x68 | data | Serbian | Italy |
| RT_GROUP_ICON | 0x26f62c0 | 0x76 | data | Serbian | Italy |
| RT_GROUP_ICON | 0x2702c58 | 0x76 | data | Serbian | Italy |
| RT_VERSION | 0x2707188 | 0x1f8 | data | | |
| None | 0x2704de0 | 0xa | data | | |

### Imports

| DLL | Import |
|---|---|
| KERNEL32.dll | CreateHardLinkA, CallNamedPipeW, GetCommConfig, GetConsoleAliasesA, GetWindowsDirectoryA, FindResourceExA, GlobalAlloc, LoadLibraryW, CreateEventA, GetConsoleAliasExesLengthW, GetStringTypeExW, GetExitCodeProcess, lstrcpynW, EnumSystemCodePagesA, GetFileAttributesW, LocalReAlloc, WriteConsoleW, GetBinaryTypeA, MultiByteToWideChar, SetLastError, FindCloseChangeNotification, VirtualAlloc, GetFileType, WriteProfileSectionW, FreeEnvironmentStringsW, GetPrivateProfileSectionA, GetStringTypeW, EnumDateFormatsW, FindAtomW, DeleteTimerQueueTimer, GlobalAddAtomW, OpenFileMappingA, LCMapStringW, OpenJobObjectA, GetProcAddress, GetStartupInfoW, HeapAlloc, GetLastError, HeapFree, GetModuleHandleW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, InterlockedDecrement, Sleep, HeapSize, ExitProcess, SetUnhandledExceptionFilter, WriteFile, GetStdHandle, GetModuleFileNameA, GetModuleFileNameW, GetEnvironmentStringsW, GetCommandLineW, SetHandleCount, GetStartupInfoA, DeleteCriticalSection, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, IsDebuggerPresent, LeaveCriticalSection, EnterCriticalSection, HeapReAlloc, RaiseException, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LoadLibraryA, InitializeCriticalSectionAndSpinCount, RtlUnwind, GetModuleHandleA, LCMapStringA, WideCharToMultiByte, GetStringTypeA, GetLocaleInfoA |
| USER32.dll | NotifyWinEvent, LoadMenuW, GetMenuInfo, ValidateRect, ArrangeIconicWindows |
| GDI32.dll | GetGlyphIndicesA |
| ADVAPI32.dll | MapGenericMask |

### Possible Origin

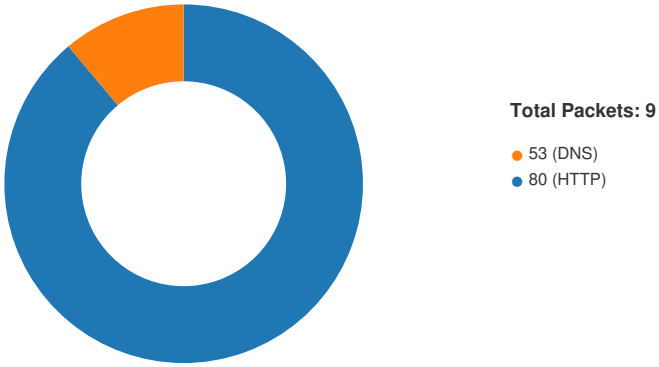
| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| Serbian | Italy |  |

## Network Behavior

### Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 192.168.2.45.44.43.1749695802033203 03/15/23-14:40:37.858863 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49695 | 80 | 192.168.2.4 | 5.44.43.17 |

## Network Port Distribution




## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Mar 15, 2023 14:40:37.787641048 CET | 49695 | 80 | 192.168.2.4 | 5.44.43.17 |
| Mar 15, 2023 14:40:37.841355085 CET | 80 | 49695 | 5.44.43.17 | 192.168.2.4 |
| Mar 15, 2023 14:40:37.841609001 CET | 49695 | 80 | 192.168.2.4 | 5.44.43.17 |
| Mar 15, 2023 14:40:37.858863115 CET | 49695 | 80 | 192.168.2.4 | 5.44.43.17 |
| Mar 15, 2023 14:40:37.912709951 CET | 80 | 49695 | 5.44.43.17 | 192.168.2.4 |
| Mar 15, 2023 14:40:37.913563967 CET | 80 | 49695 | 5.44.43.17 | 192.168.2.4 |
| Mar 15, 2023 14:40:37.913654089 CET | 49695 | 80 | 192.168.2.4 | 5.44.43.17 |
| Mar 15, 2023 14:40:37.926760912 CET | 49695 | 80 | 192.168.2.4 | 5.44.43.17 |
| Mar 15, 2023 14:40:37.980429888 CET | 80 | 49695 | 5.44.43.17 | 192.168.2.4 |
| Mar 15, 2023 14:40:57.963377953 CET | 49696 | 80 | 192.168.2.4 | 31.41.44.108 |
| Mar 15, 2023 14:41:00.968698025 CET | 49696 | 80 | 192.168.2.4 | 31.41.44.108 |
| Mar 15, 2023 14:41:06.971541882 CET | 49696 | 80 | 192.168.2.4 | 31.41.44.108 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Mar 15, 2023 14:39:17.005433083 CET | 56572 | 53 | 192.168.2.4 | 8.8.8.8 |
| Mar 15, 2023 14:39:17.028251886 CET | 53 | 56572 | 8.8.8.8 | 192.168.2.4 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|
| Mar 15, 2023 14:39:17.005433083 CET | 192.168.2.4 | 8.8.8.8 | 0xa670 | Standard query (0) | checklist.skype.com | A (IP address) | IN (0x0001) | false |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| Mar 15, 2023 14:39:17.028251886 CET | 8.8.8.8 | 192.168.2.4 | 0xa670 | Name error (3) | checklist.skype.com | none | none | A (IP address) | IN (0x0001) | false |

## HTTP Request Dependency Graph

- 5.44.43.17

## Statistics

No statistics

## System Behavior

### Analysis Process: server.exe PID: 3536, Parent PID: 3528

| General | |
|---|---|
| Target ID: | 0 |
| Start time: | 14:39:04 |
| Start date: | 15/03/2023 |
| Path: | C:\Users\user\Desktop\server.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\server.exe |
| Imagebase: | 0x400000 |
| File size: | 316928 bytes |
| MD5 hash: | 768928D17E8D3489407B540DBAD4A770 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.568856386.0000000002E48000.00000040.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.459546153.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.459546153.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.459546153.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.568965498.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.568965498.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.568965498.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.460026895.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.460026895.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.460026895.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.459923049.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.459923049.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.459923049.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.568790164.0000000002C80000.00000040.00001000.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.459750539.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.459750539.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.459750539.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.459944740.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.459944740.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.459944740.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.459896893.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.459896893.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.459896893.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.459783978.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.459783978.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.459783978.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.460044843.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.460044843.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.460044843.0000000005258000.00000004.00000020.00020000.00000000.sdmp, Author: unknown |
| Reputation: | low |

## File Activities

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

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

# Disassembly

**No disassembly**