ID: 827617
Sample Name: server.exe
Cookbook: default.jbs
Time: 07:21:06
Date: 16/03/2023
Version: 37.0.0 Beryl

Table of Contents

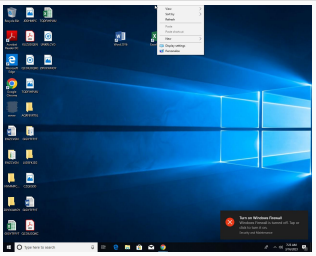
Windows Analysis Report

server.exe

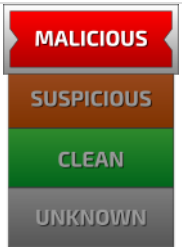
Overview

General Information

Sample Name:	server.exe
Analysis ID:	827617
MD5:	a4071382a33b…
SHA1:	4eb7f936efe97…
SHA256:	04234564fe449..
Tags:	agenziaentrate exe gozi isfb mef mise ursnif
Infos:	



Detection



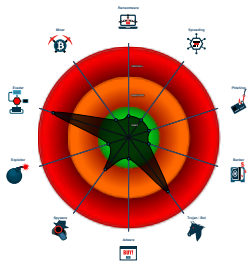
Ursnif

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- server.exe (PID: 5084 cmdline: C:\Users\user\Desktop\server.exe MD5: A4071382A33BB9FA55FF8BF8B111BC39)
- **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/zREoXS4YDyuxKi/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
00000000.00000003.437821342.00000000054A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.437821342.00000000054A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$a1: /C ping localhost -n %u && del "%s" • 0xea8:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xf00:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xa9c:$a5: filename="%.4u.%lu" • 0x63a:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x876:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xbb7:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe6d:$a9: &whoami=%s • 0xe56:$a10: %u.%u_%u_%u_x%u • 0xd63:$a11: size=%u&hash=0x%08x • 0xb1d:$a12: &uptime=%u • 0x6fb:$a13: %systemroot%\system32\c_1252.nls • 0x1298:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.437821342.00000000054A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x63a:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xa68:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xcf2:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd96:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1ca0:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.437852108.00000000054A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.437852108.00000000054A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$a1: /C ping localhost -n %u && del "%s" • 0xea8:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xf00:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xa9c:$a5: filename="%.4u.%lu" • 0x63a:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x876:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xbb7:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe6d:$a9: &whoami=%s • 0xe56:$a10: %u.%u_%u_%u_x%u • 0xd63:$a11: size=%u&hash=0x%08x • 0xb1d:$a12: &uptime=%u • 0x6fb:$a13: %systemroot%\system32\c_1252.nls • 0x1298:$a14: IE10RunOnceLastShown_TIMESTAMP

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 03/16/23-07:23:24.710750
SID:	2033203
Source Port:	49695
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 5.44.43.17

Timestamp:	192.168.2.45.44.43.1749695802033204 03/16/23-07:23:24.710750
SID:	2033204
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

Multi AV Scanner detection for domain / URL

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 (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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

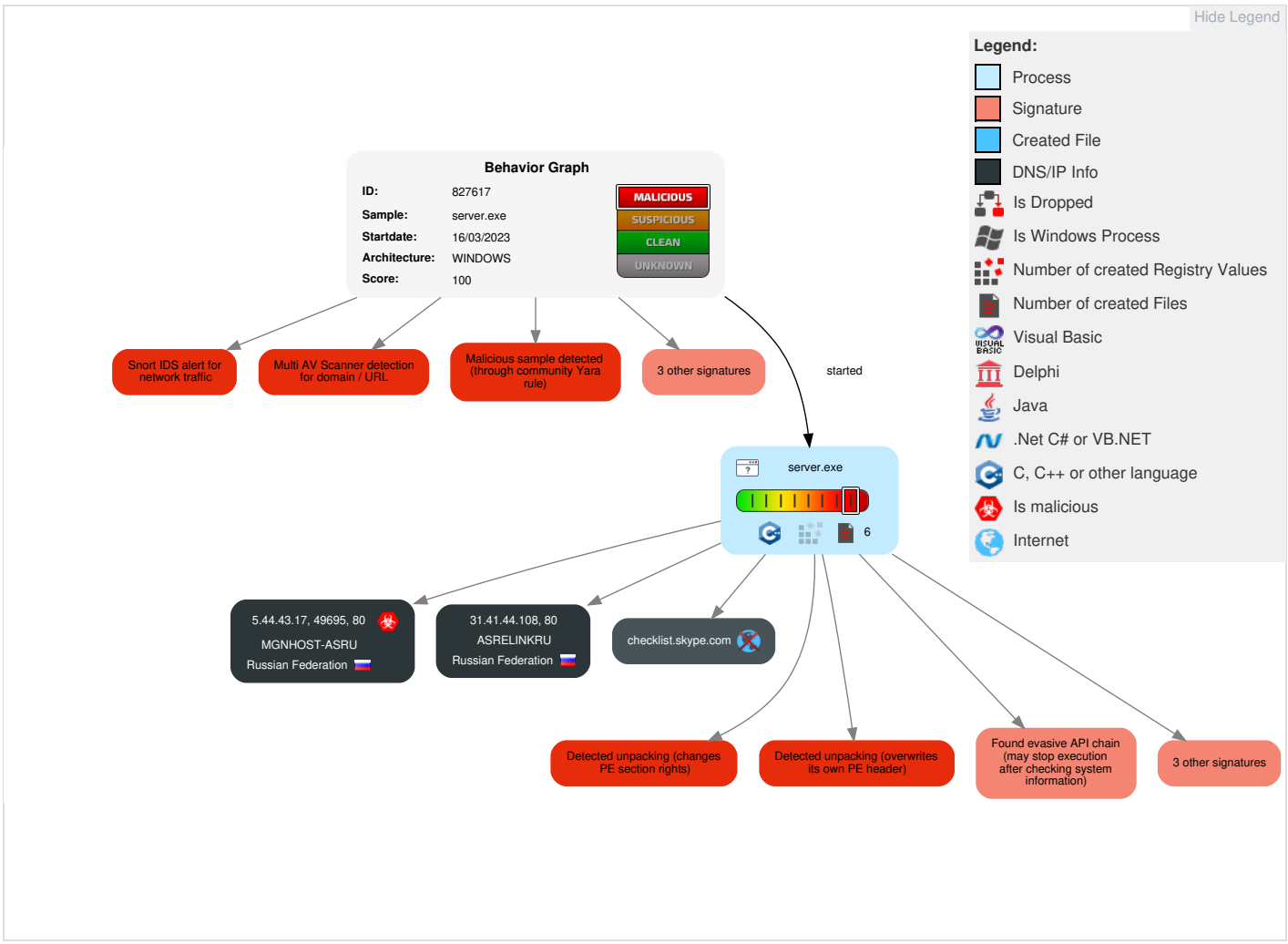
Remote Access Functionality

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Windows Management Instrumentation	Path Interception	Path Interception	1 Virtualization/Sandbox Evasion	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 1 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	Data from Removable Media	Exfiltration Over Bluetooth	2 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)	2 1 Software Packing	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System 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 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

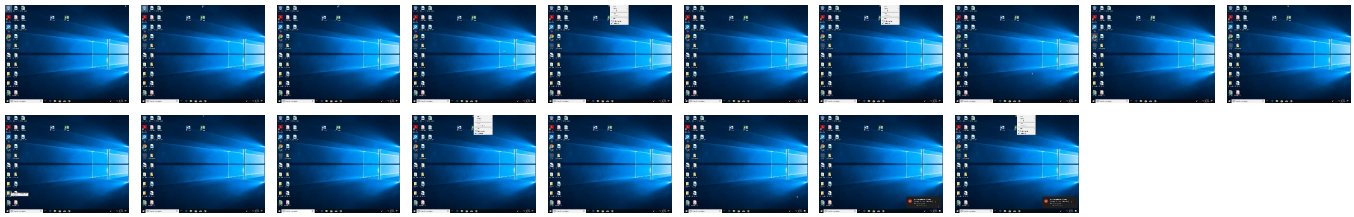
Behavior Graph



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	49%	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.2cf0000.2.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://31.41.44.108/drew/kSoLH6P3P3ScRZ8VG2/ZyGmCU1Si/Pg3By2fxJOOkAR8rwi0H/T_2F0osErSjTF4ug24E/qpC0b	0%	Avira URL Cloud	safe	
http://5.44.43.17/H	0%	Avira URL Cloud	safe	
http://31.41.44.108/ows	0%	Avira URL Cloud	safe	
http://5.44.43.17/	0%	Avira URL Cloud	safe	
http://5.44.43.17/	1%	Virustotal		Browse
http://31.41.44.108/	0%	Avira URL Cloud	safe	
http://31.41.44.108/	7%	Virustotal		Browse
http://5.44.43.17/dows	0%	Avira URL Cloud	safe	
http://5.44.43.17/drew/L2Ctnat9/M34_2FbYe0ZC9ndvN_2FGmY/27aAwtqf0J/wCDEgzGms_2BItZWy/3Y988SJvsZ8d/G3	0%	Avira URL Cloud	safe	
http://5.44.43.17/drew/L2Ctnat9/M34_2FbYe0ZC9ndvN_2FGmY/27aAwtqf0J/wCDEgzGms_2BItZWy/3Y988SJvsZ8d/G3blEZDMCSE/Bi4DBDrc6fsxs_/2B3aB3ncMi0pp47wsona_/2Bg3i_2FKiTRHGjN/oHTatVB82_2Bul8/TJX3dbVMmJ11Klc61D/Pyd9ldtz9/oHshYCyo8YOqEvONS9ad/fWHuvb04Djokj2GS9tP/hFDYxrH3WbHt3WZEGKZKd7/8Da2SdLCDRHMt/cExDArjC/xj0VJZ2pcmhn5qbmTarHUT8/nHF70Bsig92/tQ.jlk	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

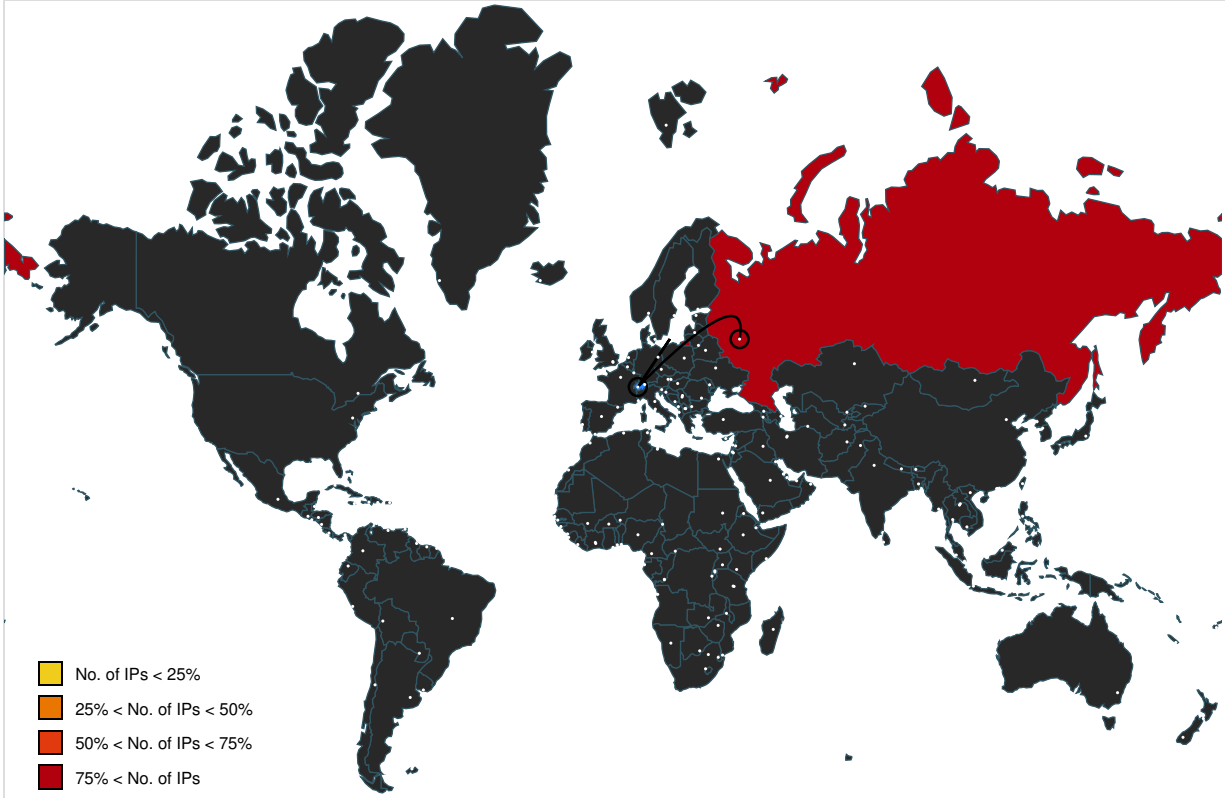
Name	Malicious	Antivirus Detection	Reputation
http://5.44.43.17/drew/L2Ctnat9/M34_2FbYe0ZC9ndvN_2FGmY/27aAwtqf0J/wCDEgzGms_2BItZWy/3Y988SJvsZ8d/G3blEZDMCSE/Bi4DBDrc6fsxs_/2B3aB3ncMi0pp47wsona_/2Bg3i_2FKiTRHGjN/oHTatVB82_2Bul8/TJX3dbVMmJ11Klc61D/Pyd9ldtz9/oHshYCyo8YOqEvONS9ad/fWHuvb04Djokj2GS9tP/hFDYxrH3WbHt3WZEGKZKd7/8Da2SdLCDRHMt/cExDArjC/xj0VJZ2pcmhn5qbmTarHUT8/nHF70Bsig92/tQ.jlk	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://31.41.44.108/ows	server.exe, 00000000.00000002.560887520.0000000002D6C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://31.41.44.108/drew/kSoLH6P3P3ScRZ8VG2/ZyGmCU1Si/Pg3By2fxJOOkAR8rwi0H/T_2F0osErSjTF4ug24E/qpC0b	server.exe, 00000000.00000002.560887520.0000000002DB5000.00000004.00000020.00020000.00000000.sdmp, server.exe, 00000000.00000002.560887520.0000000002D6C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://5.44.43.17/	server.exe, 00000000.00000002.560887520.0000000002D6C000.00000004.00000020.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://5.44.43.17/H	server.exe, 00000000.00000002.560887520.0000000002D6C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://checklist.skype.com/drew/t0_2F8jI1aC786/3pDAJvqTmNvXKWVK8YEK3/dSLDX7_2Bak45Arz/NG3260JY92AIOa	server.exe, 00000000.00000002.560887520.0000000002D6C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://31.41.44.108/	server.exe, 00000000.00000002.560887520.0000000002D6C000.00000004.00000020.00020000.00000000.sdmp	false	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://5.44.43.17/dows	server.exe, 00000000.00000002.560887520.0000000002D6C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://5.44.43.17/drew/L2Ctnat9/M34_2FbYe0ZC9ndvN_2FGmY/27aAwtqf0J/wCDEgzGms_2BItZWy/3Y988SJvsZ8d/G3	server.exe, 00000000.00000002.560824916.0000000002D4A000.00000004.00000020.00020000.00000000.sdmp, server.exe, 00000000.00000002.560887520.0000000002D6C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://31.41.	server.exe, 00000000.00000002.561015752.00000000048DC000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

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:	827617
Start date and time:	2023-03-16 07:21:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 48s
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 • EGA enabled • HDC enabled • 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: 9.6% (good quality ratio 9.6%) • Quality average: 89% • Quality standard deviation: 15.4%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • 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):	6.1349432521483696
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	server.exe
File size:	307200
MD5:	a4071382a33bb9fa55ff8bf8b111bc39
SHA1:	4eb7f936efe97a88aad9d38452829cd63a3624b2
SHA256:	04234564fe449d51f7e685455fcfafb3b7721a0b7d1551e3a370f579a3530e04
SHA512:	43a54adc868158e342419a4102e4a58a7556a2670f65991a4b71a23ccdc881edd30919a42dfcd2f8730d4e2117663936ea345dc467b43ebb7d48154fb792a19b
SSDEEP:	3072:HntJSBTLHSkg+3ukUWAKi1KPx5pZziCtyF4kWzbmgkONlfQKH:HtJQL1737AKwKJ5pZziB4kvlj
TLSH:	10642B0393E1BD85F92A8B729E1FCAF8765EF5508E09776922289F1F44B0277D263710
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.c. .0. .0. .0.r.0. .0.r.0. .0.r.0. .0..j0. .0. .0. .0.r.0. .0.r.0. .0.r.0. .0Rich. .0.....PE..L...@r.b.....

File Icon

Icon Hash:	a4a4809484aca4e2

Static PE Info

General

Entrypoint:	0x404d88
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:	0x62867240 [Thu May 19 16:37:20 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:	0011bb4cb3dd2f1183b8c6c4581099ab

Entrypoint Preview

Instruction
call 00007F78A0CADE74h
jmp 00007F78A0CABEBEh
mov edi, edi
push ecx
mov dword ptr [ecx], 0040124Ch
call 00007F78A0CADEF7h
pop ecx
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, ecx
call 00007F78A0CAC028h
test byte ptr [ebp+08h], 00000001h

Instruction
je 00007F78A0CAC049h
push esi
call 00007F78A0CAC2F3h
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 00007F78A0CAC049h
mov edi, dword ptr [ebp+0Ch]
cmp edi, ebx
jnbe 00007F78A0CAC05Dh
call 00007F78A0CAE15Ch
push 00000016h
pop esi
mov dword ptr [eax], esi
push ebx
push ebx
push ebx
push ebx
push ebx
call 00007F78A0CAE0E5h
add esp, 14h
mov eax, esi
jmp 00007F78A0CAC072h
mov esi, dword ptr [ebp+10h]
cmp esi, ebx
jne 00007F78A0CAC046h
mov byte ptr [ecx], bl
jmp 00007F78A0CAC01Ch
mov edx, ecx
mov al, byte ptr [esi]
mov byte ptr [edx], al
inc edx
inc esi
cmp al, bl
je 00007F78A0CAC045h
dec edi
jne 00007F78A0CAC035h
cmp edi, ebx
jne 00007F78A0CAC052h
mov byte ptr [ecx], bl
call 00007F78A0CAE121h
push 00000022h
pop ecx
mov dword ptr [eax], ecx
mov esi, ecx
jmp 00007F78A0CAC003h
xor eax, eax
pop edi

Instruction
pop esi
pop ebx
pop ebp
ret
push 0000000Ch
push 0040EE10h
call 00007F78A0CADBD6h
and dword ptr [ebp-1Ch], 00000000h
mov esi, dword ptr [ebp+08h]
cmp esi, dword ptr [02AE85F0h]
jnbe 00007F78A0CAC064h
push 00000004h
call 00007F78A0CAE27Eh
pop ecx
and dword ptr [ebp+00h], 00000000h

Rich Headers

Programming Language:	• [C++] VS2008 build 21022 • [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf0bc	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26e9000	0x1d550	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2707000	0xa34	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11b0	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	0x2d70	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x16c	.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	0xe8f0	0xea00	False	0.5854867788461539	data	6.74566977698935	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x10000	0x26d8744	0x17200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x26e9000	0x1d550	0x1d600	False	0.39934341755319147	data	4.477676246646998	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2707000	0x7878	0x7a00	False	0.07479508196721311	data	0.9257939540365804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x2702bf0	0x330	Device independent bitmap graphic, 48 x 96 x 1, image size 0		
RT_CURSOR	0x2702f20	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x2703078	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_CURSOR	0x2703f20	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_CURSOR	0x27047c8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_CURSOR	0x2704d60	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x2704e90	0xb0	Device independent bitmap graphic, 16 x 32 x 1, image size 0		
RT_ICON	0x26e9b10	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Serbian	Italy
RT_ICON	0x26ea9b8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Serbian	Italy
RT_ICON	0x26eb260	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Serbian	Italy
RT_ICON	0x26eb928	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Serbian	Italy
RT_ICON	0x26ebe90	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Serbian	Italy
RT_ICON	0x26ee438	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Serbian	Italy
RT_ICON	0x26ef4e0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Serbian	Italy
RT_ICON	0x26ef9b0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Serbian	Italy
RT_ICON	0x26f0858	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Serbian	Italy
RT_ICON	0x26f1100	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Serbian	Italy
RT_ICON	0x26f17c8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Serbian	Italy
RT_ICON	0x26f1d30	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Serbian	Italy
RT_ICON	0x26f42d8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Serbian	Italy
RT_ICON	0x26f5380	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Serbian	Italy
RT_ICON	0x26f5d08	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Serbian	Italy
RT_ICON	0x26f61e8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Serbian	Italy
RT_ICON	0x26f7090	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Serbian	Italy
RT_ICON	0x26f7938	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Serbian	Italy
RT_ICON	0x26f7ea0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Serbian	Italy
RT_ICON	0x26fa448	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Serbian	Italy
RT_ICON	0x26fb4f0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Serbian	Italy
RT_ICON	0x26fbe78	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Serbian	Italy
RT_ICON	0x26fc348	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Serbian	Italy
RT_ICON	0x26fd1f0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Serbian	Italy
RT_ICON	0x26fda98	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Serbian	Italy
RT_ICON	0x26fe160	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Serbian	Italy
RT_ICON	0x26fe6c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Serbian	Italy
RT_ICON	0x2700c70	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Serbian	Italy

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2701d18	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Serbian	Italy
RT_ICON	0x27026a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Serbian	Italy
RT_DIALOG	0x2705160	0x86	data		
RT_STRING	0x27051e8	0x2be	data		
RT_STRING	0x27054a8	0x492	data		
RT_STRING	0x2705940	0x5c6	data		
RT_STRING	0x2705f08	0x118	data		
RT_STRING	0x2706020	0x52a	data		
RT_ACCELERATOR	0x2702b80	0x48	data	Serbian	Italy
RT_ACCELERATOR	0x2702bc8	0x18	data	Serbian	Italy
RT_GROUP_CURSOR	0x2703050	0x22	data		
RT_GROUP_CURSOR	0x2704d30	0x30	data		
RT_GROUP_CURSOR	0x2704f40	0x22	data		
RT_GROUP_ICON	0x26fc2e0	0x68	data	Serbian	Italy
RT_GROUP_ICON	0x26ef948	0x68	data	Serbian	Italy
RT_GROUP_ICON	0x26f6170	0x76	data	Serbian	Italy
RT_GROUP_ICON	0x2702b08	0x76	data	Serbian	Italy
RT_VERSION	0x2704f68	0x1f8	data		
None	0x2702be0	0xa	data		

Imports

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

Possible Origin

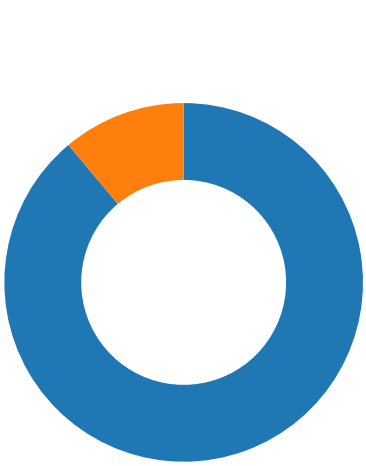
Language of compilation system	Country where language is spoken	Map
Serbian	Italy	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.45.44.43.1749695802033203 03/16/23-07:23:24.710750	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49695	80	192.168.2.4	5.44.43.17
192.168.2.45.44.43.1749695802033204 03/16/23-07:23:24.710750	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	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 16, 2023 07:23:24.650625944 CET	49695	80	192.168.2.4	5.44.43.17
Mar 16, 2023 07:23:24.707762957 CET	80	49695	5.44.43.17	192.168.2.4
Mar 16, 2023 07:23:24.707907915 CET	49695	80	192.168.2.4	5.44.43.17
Mar 16, 2023 07:23:24.710750103 CET	49695	80	192.168.2.4	5.44.43.17
Mar 16, 2023 07:23:24.763972044 CET	80	49695	5.44.43.17	192.168.2.4
Mar 16, 2023 07:23:24.765341997 CET	80	49695	5.44.43.17	192.168.2.4
Mar 16, 2023 07:23:24.765438080 CET	49695	80	192.168.2.4	5.44.43.17
Mar 16, 2023 07:23:24.768033028 CET	49695	80	192.168.2.4	5.44.43.17
Mar 16, 2023 07:23:24.822140932 CET	80	49695	5.44.43.17	192.168.2.4
Mar 16, 2023 07:23:44.814861059 CET	49696	80	192.168.2.4	31.41.44.108
Mar 16, 2023 07:23:47.821590900 CET	49696	80	192.168.2.4	31.41.44.108
Mar 16, 2023 07:23:53.837632895 CET	49696	80	192.168.2.4	31.41.44.108

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 16, 2023 07:22:03.757394075 CET	56572	53	192.168.2.4	8.8.8.8
Mar 16, 2023 07:22:03.788410902 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 16, 2023 07:22:03.757394075 CET	192.168.2.4	8.8.8.8	0xe6b9	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 16, 2023 07:22:03.788410902 CET	8.8.8.8	192.168.2.4	0xe6b9	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: 5084, Parent PID: 3528

General

Target ID:	0
Start time:	07:21:56
Start date:	16/03/2023
Path:	C:\Users\user\Desktop\server.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\server.exe
Imagebase:	0x400000
File size:	307200 bytes
MD5 hash:	A4071382A33BB9FA55FF8BF8B111BC39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437821342.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437821342.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437821342.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437852108.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437852108.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437852108.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437607337.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437607337.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437607337.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437902952.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437902952.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437902952.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437680280.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437680280.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437680280.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437880464.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437880464.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437880464.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.436425972.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.436425972.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.436425972.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.561151548.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.561151548.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.561151548.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.560851312.0000000002D56000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.560764513.0000000002B60000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437645117.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437645117.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437645117.00000000054A8000.00000004.00000020.00020000.00000000.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