ID: 830620
Sample Name: server.exe
Cookbook: default.jbs
Time: 14:47:25
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

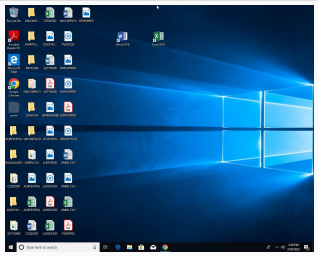
Windows Analysis Report

server.exe

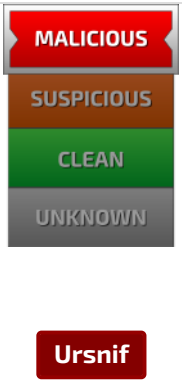
Overview

General Information

Sample Name:	server.exe
Analysis ID:	830620
MD5:	0fcb834306b46..
SHA1:	34d67f8911512..
SHA256:	b97cfd0ea14f3...
Tags:	agenziaentrate exe gozi isfb mef mise ursnif
Infos:	



Detection



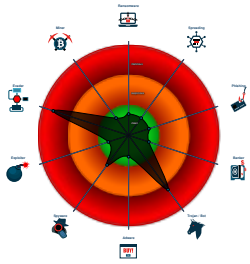
Ursnif

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...
- 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...
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- server.exe (PID: 5684 cmdline: C:\Users\user\Desktop\server.exe MD5: 0FCB834306B465D8998C654A5D4C3727)
- **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://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/gozi-italian-shellcode-dancehttps://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"ScCjtIu/chsReaToemavuPsGfYIczuvCBclhySG8/AhfUJMnvau4hmaBPIAXScUh9/secJMcCpqd5yeayd2fJdEc3ETZJfeY55SskXGIyxmn6sJL8WH2YF95GitV+tnd52epRBd8/snxdFtGg4Pgf9kxQsW/ySpD96hQxlGzGgDApS0E54E54SLEBTqihX3FWN2//mDaDIJuoFz7lt0whvCg/8gXPBf/s2nkXoRwyyqXguvwDcw9IZEu1NT1qqIwpXL9DGlddaMvwfXTGOLIkQX35RsJJDpP1V5Mcgc+c1nBRPKqGQz+NUtKDBiyp0RXMK3jDdMGWvimLl80kvMkvSd8fQXtWRcZ7DCuQwrQxkXo=",
  "c2_domain": [
    "checklist.skype.com",
    "62.173.142.81",
    "193.233.175.113",
    "109.248.11.184",
    "212.109.218.26",
    "185.68.93.7"
  ],
  "botnet": "7715",
  "server": "50",
  "serpent_key": "xeaLJj1BwSDpjIfH",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.494473837.0000000002B88000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.494473837.0000000002B88000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.494473837.0000000002B88000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$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\ • 0x1cc0:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.494317302.0000000002B88000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.494317302.0000000002B88000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$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 M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 62.173.142.81

Timestamp:	192.168.2.462.173.142.8149744802033204 03/20/23-14:50:08.876775
SID:	2033204
Source Port:	49744
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 (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

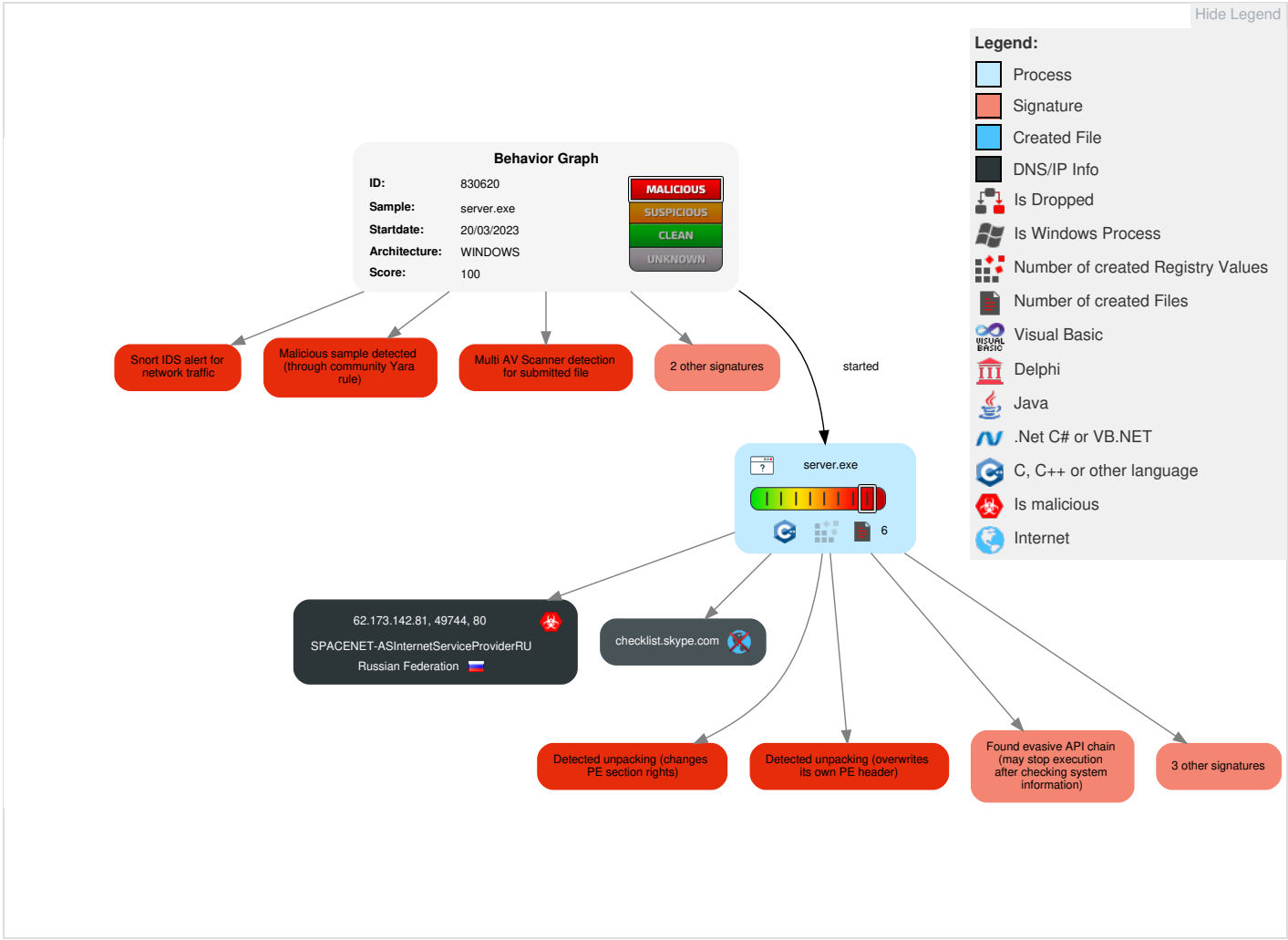
Remote Access Functionality

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 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Non-Application Layer Protocol	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	2 1 Software Packing	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 2 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 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	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 1 4 System Information 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

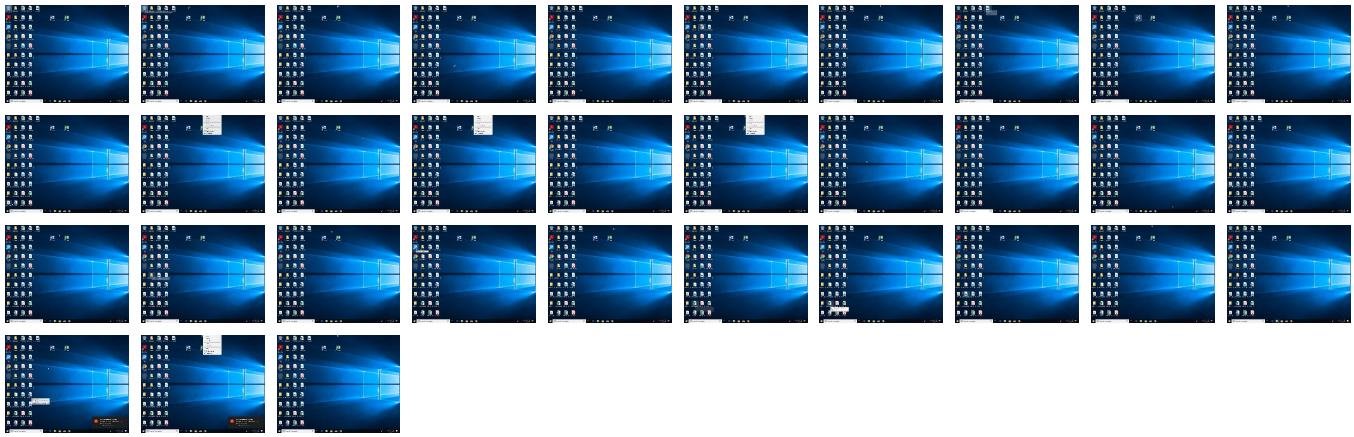
Behavior Graph



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	42%	Virustotal		Browse
server.exe	36%	ReversingLabs	Win32.Trojan.Generic	
server.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.server.exe.5b0000.2.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://62.173.142.81/drew/I7U6Mmh_2/FlKCcCvddS2lkyhwmZhl/_2BnhFHclgzHZzSm1pz/lqwUwcf_2FOd8gS4FMlTC_/2BvcUI51vMc8r/suycgkYX/cZV8UZtrltZ4gcEVM5eiX0K/R8EhhQWcO2/VNo_2Fqah4SvEVbxz/wWOUzBOqDpod/WDVr2wrvR3Y/HsF0WzspqprqGt/jOCmPbtKRTDFN85npSKPi/bt89T8vUv5SwQ97g/AKkdy2tkCMuBk2l/mwXR08zcp_2FWg_2Fs/Xeh1WbyLh/PXYBkYg4EIsUFknKnI2W/_2FJmsR6G_2F/BQ3Eo_2F/X.jlk	0%	Avira URL Cloud	safe	
http://62.173	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

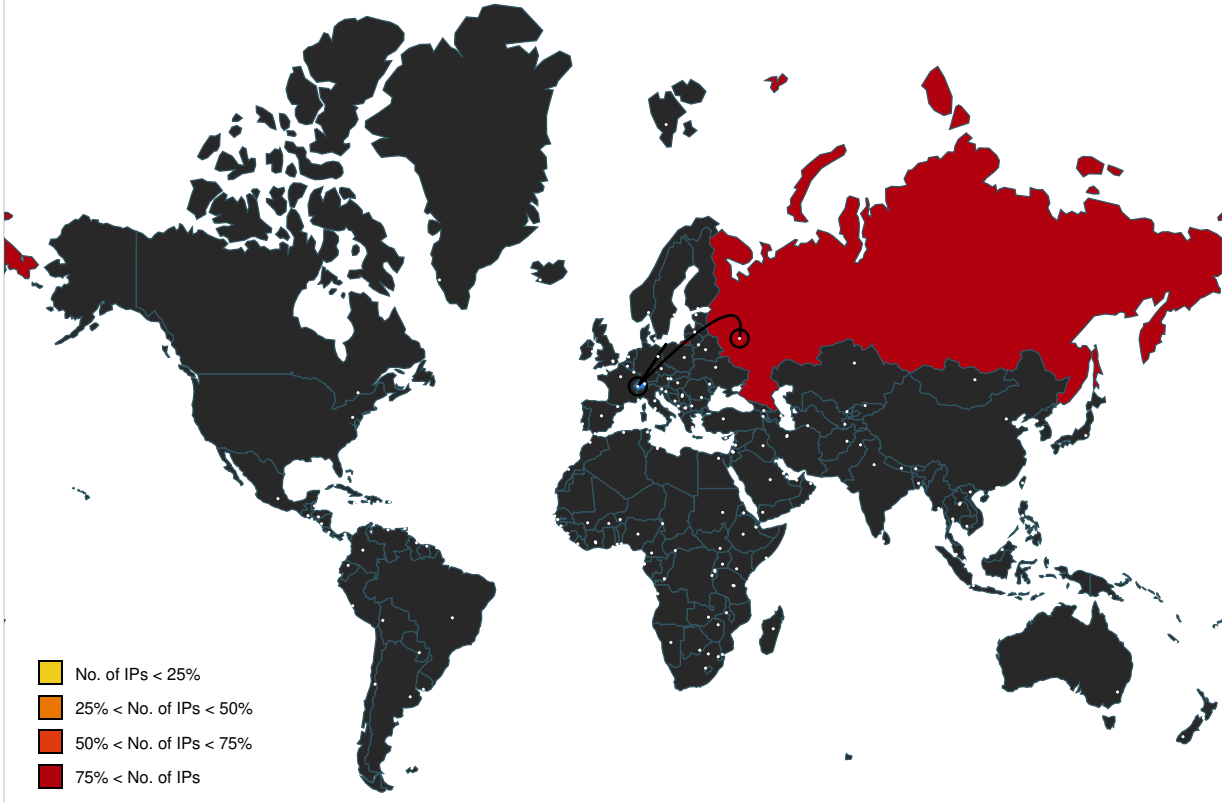
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://62.173.142.81/drew/I7U6Mmh_2/FlKCcCvddS2lkyhwmZhl/_2BnhFHclgzHZzSm1pz/lqwUwcf_2FOd8gS4FMlTC_/2BvcUI51vMc8r/suycgkYX/cZV8UZtrltZ4gcEVM5eiX0K/R8EhhQWcO2/VNo_2Fqah4SvEVbxz/wWOUzBOqDpod/WDVr2wrvR3Y/HsF0WzspqprqGt/jOCmPbtKRTDFN85npSKPi/bt89T8vUv5SwQ97g/AKkdy2tkCMuBk2l/mwXR08zcp_2FWg_2Fs/Xeh1WbyLh/PXYBkYg4EIsUFknKnI2W/_2FJmsR6G_2F/BQ3Eo_2F/X.jlk	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://62.173	server.exe, 00000000.00000002.579878566.00000000022CC000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.173.142.81	unknown	Russian Federation		34300	SPACENET-ASInternetServiceProviderRU	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830620
Start date and time:	2023-03-20 14:47:25 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
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:	26
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@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 100%) • Quality average: 89% • Quality standard deviation: 15.4%
HCA Information:	• Successful, ratio: 93% • 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, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, login.live.com, store-images.s-microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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):	6.801149761040853
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:	182272
MD5:	0fcb834306b465d8998c654a5d4c3727
SHA1:	34d67f89115124d042f65cff8f16a5508e8336c3
SHA256:	b97cfd0ea14f390894948861cacafbad2f88767d52477e339e2c0a6e4316793b
SHA512:	d95647ffd2017fedcdcdc3db4fad352613a82b10704d97c1bc91dd1375aa0f1c3ca2ce0395ecdc77a545acfcd5c5cca244230e57b3cad06b7ed70ec416f773c7
SSDEEP:	3072:2bKsm0/YwL+NqvT+u8TEaYDSj6krWt+3j4XBps2Q:d30QO+udabGTEw
TLSH:	54049ED2A2D0BC52E4128A36CE2FC2F4770DF991CE5DA766E3186B5F08BC162C56B711
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f.Q.f.Q.f.Q...Q.f.Q..4Q.f.Q...Q.f.Q..9Q.f.Q.f.Q.f.Q...Q.f.Q..0Q.f.Q..7Q.f.QRich.f.Q.....PE..L...'*.c.....

File Icon

Icon Hash:	9a8242428da282a2

Static PE Info

General

Entrypoint:	0x402f31
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE

DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x63032A27 [Mon Aug 22 07:03:03 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	b6299cf22bb1b2b906c76a98a991dd84

Entrypoint Preview
Instruction
call 00007F29B07633E0h
jmp 00007F29B0760A0Eh
mov eax, 0040D008h
ret
mov eax, dword ptr [0049D840h]
push esi
push 00000014h
pop esi
test eax, eax
jne 00007F29B0760B89h
mov eax, 00000200h
jmp 00007F29B0760B88h
cmp eax, esi
jnl 00007F29B0760B89h
mov eax, esi
mov dword ptr [0049D840h], eax
push 00000004h
push eax
call 00007F29B076348Eh
pop ecx
pop ecx
mov dword ptr [0049C820h], eax
test eax, eax
jne 00007F29B0760BA0h
push 00000004h
push esi
mov dword ptr [0049D840h], esi
call 00007F29B0763475h
pop ecx
pop ecx
mov dword ptr [0049C820h], eax
test eax, eax
jne 00007F29B0760B87h
push 0000001Ah
pop eax
pop esi
ret
xor edx, edx
mov ecx, 0040D008h
jmp 00007F29B0760B87h
mov eax, dword ptr [0049C820h]
mov dword ptr [edx+eax], ecx
add ecx, 20h
add edx, 04h
cmp ecx, 0040D288h
jl 00007F29B0760B6Ch

Instruction
push FFFFFFFEh
pop esi
xor edx, edx
mov ecx, 0040D018h
push edi
mov eax, edx
sar eax, 05h
mov eax, dword ptr [0049C720h+eax*4]
mov edi, edx
and edi, 1Fh
shl edi, 06h
mov eax, dword ptr [edi+eax]
cmp eax, FFFFFFFFh
je 00007F29B0760B8Ah
cmp eax, esi
je 00007F29B0760B86h
test eax, eax
jne 00007F29B0760B84h
mov dword ptr [ecx], esi
add ecx, 20h
inc edx
cmp ecx, 0040D078h
jl 00007F29B0760B50h
pop edi
xor eax, eax
pop esi
ret
call 00007F29B0761196h
cmp byte ptr [00000000h], 00000000h

Rich Headers

Programming Language:	• [C++] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [RES] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb84c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9f000	0xdae8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2b08	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x19c	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb1b0	0xb200	False	0.514747191011236	data	6.023722982604758	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xd000	0x9084c	0x13400	False	0.9433340097402597	data	7.842506662554348	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.paboju	0x9e000	0x96	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x9f000	0xdae8	0xdc00	False	0.4137961647727273	data	4.476519968277395	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0xab598	0x2	data		
TONIZITOHOWAPEVUMOBEM	0xaaea0	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Finland
TONIZITOHOWAPEVUMOBEM	0xaaea0	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Norway
TONIZITOHOWAPEVUMOBEM	0xaaea0	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Sweden
RT_CURSOR	0xab5a0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xab6d0	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0xab7c0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x9f680	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0x9f680	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0x9f680	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0x9ff28	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0x9ff28	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0x9ff28	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa0ff8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa0ff8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa0ff8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa18a0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa18a0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa18a0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa3e48	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa3e48	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa3e48	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa4f20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa4f20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa4f20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa5dc8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa5dc8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Norway

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa5dc8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa6490	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa6490	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa6490	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa69f8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa69f8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa69f8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa8fa0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa8fa0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa8fa0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xaa048	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xaa048	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xaa048	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xaa9d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xaa9d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xaa9d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Sweden
RT_ACCELERATOR	0xab4e0	0x78	data	Sami Lappish	Finland
RT_ACCELERATOR	0xab4e0	0x78	data	Sami Lappish	Norway
RT_ACCELERATOR	0xab4e0	0x78	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xab438	0xa8	data	Sami Lappish	Finland
RT_ACCELERATOR	0xab438	0xa8	data	Sami Lappish	Norway
RT_ACCELERATOR	0xab438	0xa8	data	Sami Lappish	Sweden
RT_GROUP_CURSOR	0xac868	0x30	data		
RT_GROUP_ICON	0xa4ef0	0x30	data	Sami Lappish	Finland
RT_GROUP_ICON	0xa4ef0	0x30	data	Sami Lappish	Norway
RT_GROUP_ICON	0xa4ef0	0x30	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xa0fd0	0x22	data	Sami Lappish	Finland
RT_GROUP_ICON	0xa0fd0	0x22	data	Sami Lappish	Norway
RT_GROUP_ICON	0xa0fd0	0x22	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xaae38	0x68	data	Sami Lappish	Finland
RT_GROUP_ICON	0xaae38	0x68	data	Sami Lappish	Norway
RT_GROUP_ICON	0xaae38	0x68	data	Sami Lappish	Sweden
RT_VERSION	0xac898	0x24c	data		
None	0xab558	0xa	data	Sami Lappish	Finland
None	0xab558	0xa	data	Sami Lappish	Norway
None	0xab558	0xa	data	Sami Lappish	Sweden
None	0xab568	0xa	data	Sami Lappish	Finland
None	0xab568	0xa	data	Sami Lappish	Norway
None	0xab568	0xa	data	Sami Lappish	Sweden
None	0xab578	0xa	data	Sami Lappish	Finland
None	0xab578	0xa	data	Sami Lappish	Norway
None	0xab578	0xa	data	Sami Lappish	Sweden
None	0xab588	0xa	data	Sami Lappish	Finland
None	0xab588	0xa	data	Sami Lappish	Norway
None	0xab588	0xa	data	Sami Lappish	Sweden

Imports

DLL	Import
KERNEL32.dll	PulseEvent, SetDefaultCommConfigA, FindFirstFileW, EnumCalendarInfoA, CopyFileExW, GetConsoleAliasExesA, _llseek, BuildCommDCBAndTimeoutsA, GetConsoleAliasA, GetCurrentProcess, InterlockedCompareExchange, GetWindowsDirectoryA, EnumTimeFormatsA, WriteFileGather, EnumResourceTypesA, ActivateActCtx, GetFirmwareEnvironmentVariableA, LoadLibraryW, Sleep, ReadConsoleInputA, GetFileAttributesW, WritePrivateProfileSectionW, TerminateProcess, IsDBCSLeadByte, lstrcmpW, GlobalUnlock, RaiseException, SetCurrentDirectoryA, SetLastError, GetProcAddress, EnterCriticalSection, GlobalGetAtomNameA, GlobalFree, OpenWaitableTimerA, LocalAlloc, FindFirstVolumeMountPointW, AddAtomA, FindNextFileA, GetModuleHandleA, GetCPInfoExA, SetCalendarInfoA, DeleteFileW, EnumCalendarInfoExA, GetLastError, DeleteFileA, GetCommandLineA, HeapSetInformation, GetStartupInfoW, LeaveCriticalSection, SetFilePointer, SetHandleCount, GetStdHandle, InitializeCriticalSectionAndSpinCount, GetFileType, DeleteCriticalSection, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, EncodePointer, DecodePointer, GetModuleHandleW, ExitProcess, WriteFile, GetModuleFileNameW, GetModuleFileNameA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, InterlockedDecrement, HeapCreate, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapFree, SetStdHandle, GetConsoleCP, GetConsoleMode, FlushFileBuffers, RtlUnwind, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapAlloc, HeapReAlloc, WriteConsoleW, MultiByteToWideChar, IsProcessorFeaturePresent, LCMapStringW, GetStringTypeW, HeapSize, CloseHandle, CreateFileW
USER32.dll	LoadMenuA

Possible Origin

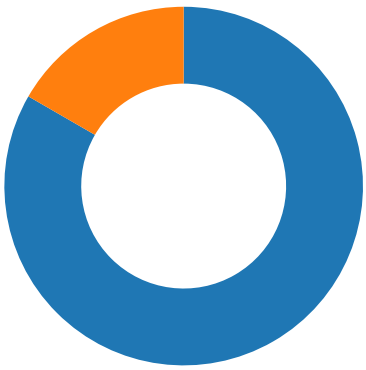
Language of compilation system	Country where language is spoken	Map
Sami Lappish	Finland	
Sami Lappish	Norway	
Sami Lappish	Sweden	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.462.173.142.81 49744802033204 03/20/23-14:50:08.876775	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49744	80	192.168.2.4	62.173.142.81

Network Port Distribution



Total Packets: 6

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 14:50:08.810525894 CET	49744	80	192.168.2.4	62.173.142.81
Mar 20, 2023 14:50:08.874392033 CET	80	49744	62.173.142.81	192.168.2.4
Mar 20, 2023 14:50:08.876282930 CET	49744	80	192.168.2.4	62.173.142.81
Mar 20, 2023 14:50:08.876775026 CET	49744	80	192.168.2.4	62.173.142.81
Mar 20, 2023 14:50:08.940011024 CET	80	49744	62.173.142.81	192.168.2.4
Mar 20, 2023 14:50:08.940210104 CET	80	49744	62.173.142.81	192.168.2.4
Mar 20, 2023 14:50:08.944226027 CET	49744	80	192.168.2.4	62.173.142.81
Mar 20, 2023 14:50:08.946094990 CET	49744	80	192.168.2.4	62.173.142.81
Mar 20, 2023 14:50:09.010911942 CET	80	49744	62.173.142.81	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 14:48:48.492964029 CET	51600	53	192.168.2.4	8.8.8.8
Mar 20, 2023 14:48:48.516079903 CET	53	51600	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 20, 2023 14:48:48.492964029 CET	192.168.2.4	8.8.8.8	0x103c	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 20, 2023 14:48:48.516079903 CET	8.8.8.8	192.168.2.4	0x103c	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 62.173.142.81

Statistics

No statistics

System Behavior

Analysis Process: server.exe PID: **5684**, Parent PID: **3528**

General

Target ID:	0
Start time:	14:48:23
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\server.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\server.exe
Imagebase:	0x400000
File size:	182272 bytes
MD5 hash:	0FCB834306B465D8998C654A5D4C3727

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: 00000000.00000003.494473837.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494473837.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494473837.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494317302.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494317302.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494317302.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494814217.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494814217.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494814217.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.579607951.00000000005E6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494422927.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494422927.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494422927.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.579371667.0000000000550000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494393831.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494393831.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494393831.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494448728.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494448728.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494448728.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494505599.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494505599.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494505599.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.580003792.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.580003792.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.580003792.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494360252.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494360252.0000000002B88000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494360252.0000000002B88000.00000004.00000020.00020000.00000000.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