ID: 826308
Sample Name: server.exe
Cookbook: default.jbs
Time: 15:59:46
Date: 14/03/2023
Version: 37.0.0 Beryl

Table of Contents

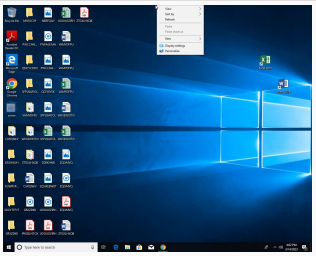
Windows Analysis Report

server.exe

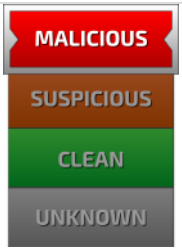
Overview

General Information

Sample Name:	server.exe
Analysis ID:	826308
MD5:	8f092511c91bf…
SHA1:	dc67d8f55a659..
SHA256:	9261b47b4fd67..
Tags:	agenziaentrate exe gozi isfb mef mise ursnif
Infos:	



Detection



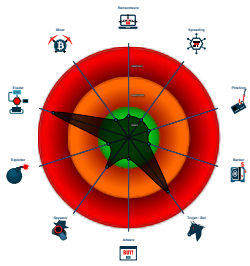
Ursnif

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

Signatures

- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- 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…

Classification



Process Tree

- **System is w10x64**
- server.exe (PID: 5540 cmdline: C:\Users\user\Desktop\server.exe MD5: 8F092511C91BFC1F2516E420739A7967)
- **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":
"2cHitNE2khtX8MPowN3OuEF+nIJiRQvDS0CByWczHAmlx7InAyPYhqz4W4BdwOQhPXM+cNmTKZrjXkeaD1W/JReU+0QfnRaZLQzMkbf/6hntYeJLN9kVYaXwOSubcfndLd/IRF3zHco37HpGyfr/fx+pYcUFQUpDPSBwxpcqOgAGHU0E
LflY4Wg7JTro/JzFnlTf/qZRLIK0F3z73FRQhjYYH8ldszb/+eADX8rn6ird+QrxU0NdIdel89Q7IsIw6+kcDa/Uh8s29ZPGfilEQcNwZsKPhbL1nQo8gRUU9nCXs8mGibasUhj7JSzvSDXMce/idAcO3inRDu0kAkFPSSWXYHucvOV7U
qKvwvqosHo=",
  "c2_domain": [
    "checklist.skype.com",
    "62.173.142.51",
    "94.103.183.153",
    "193.233.175.111",
    "109.248.11.145",
    "31.41.44.106",
    "191.96.251.201"
  ],
  "botnet": "7713",
  "server": "50",
  "serpent_key": "rqDYWFa4uPXuBFMj",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.494639050.0000000002C68000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.494639050.0000000002C68000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.494639050.0000000002C68000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$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\ • 0x1ce8:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.494532027.0000000002C68000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.494532027.0000000002C68000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$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: 192.168.2.5 - Destination IP: 62.173.142.51

Timestamp:	192.168.2.562.173.142.5149680802033203 03/14/23-16:02:33.550566
SID:	2033203
Source Port:	49680
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

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

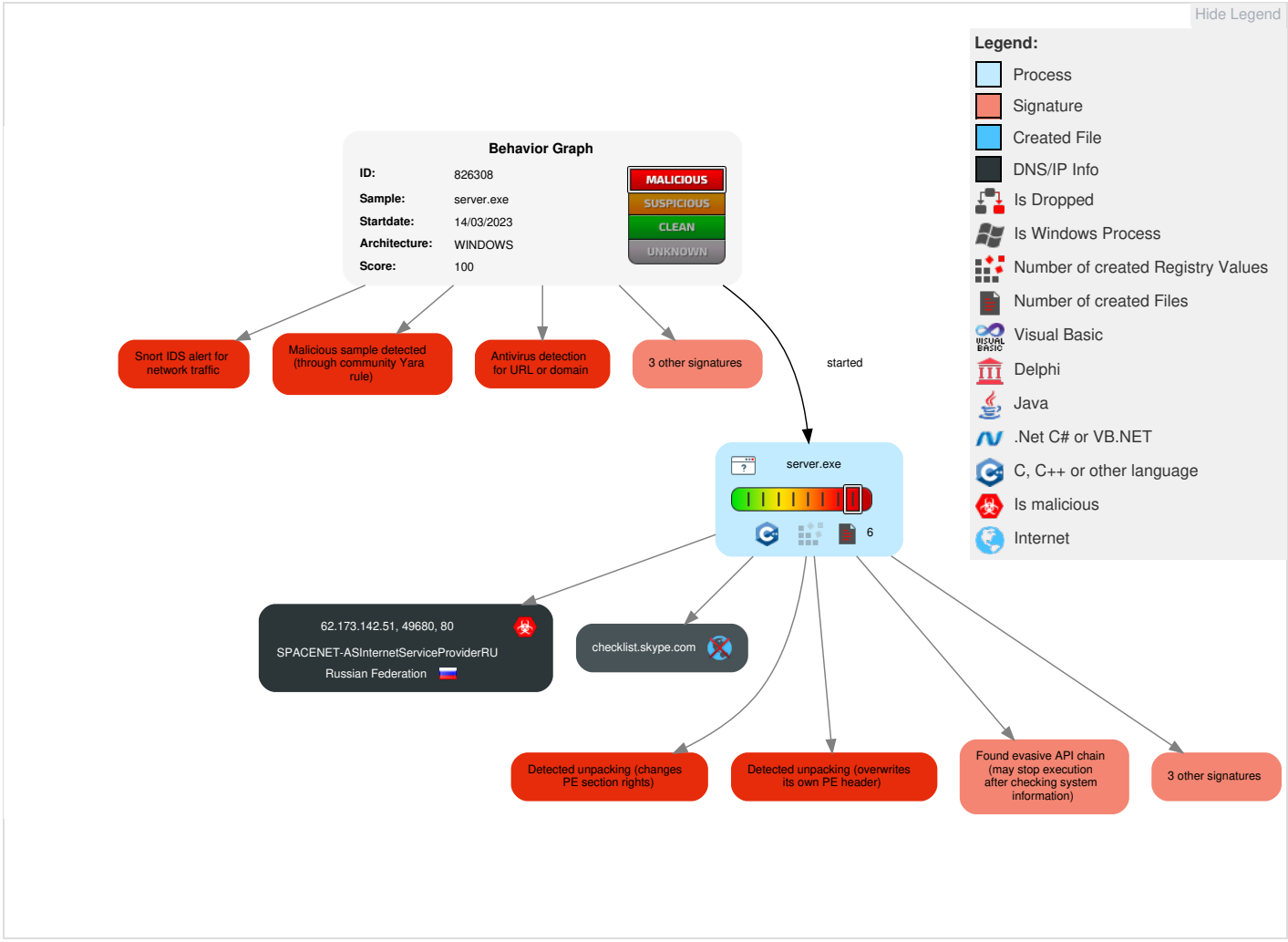
Remote Access Functionality

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	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 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	32%	ReversingLabs	Win32.Trojan.Generic	
server.exe	43%	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.680000.2.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://62.173.142.51/	2%	Virustotal		Browse
http://62.173.142.51/drew/kjSOZcm1saisXVulw/nMJdjuoxI5rY/D8rf0rwxZvy/xTo4u6qyfG2cqh/DrEm9eSMLtL3Mt_2	100%	Avira URL Cloud	malware	
http://62.173.142.51/drew/kjSOZcm1saisXVulw/nMJdjuoxI5rY/D8rf0rwxZvy/xTo4u6qyfG2cqh/DrEm9eSMLtL3Mt_2BWc8v/UHxdAMkcyeaROQd9/EwiLplzlm9gCiDQ/KqEVG_2BN1u2apPrXD/iYwyB9P6y/3dh1O1SBALUj6nSMRJfH/HHlM5d4xQO9d95rkA_2/Bt59zcQMsfJpOgJC8GeSrH/5REGnF8guLwya/xQ1cfd2Y/w3tCRH4bjXIzu_2B_2F_2B5/MmfV_2FK_2/B5ux_2BgxJ6omqMfT/iSBh1mrWB9_2/BRaJgBOq4gEVdF7OIVd_2B/4.jlk	100%	Avira URL Cloud	malware	
http://62.173	0%	Virustotal		Browse
http://62.173.142.51/	100%	Avira URL Cloud	malware	
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

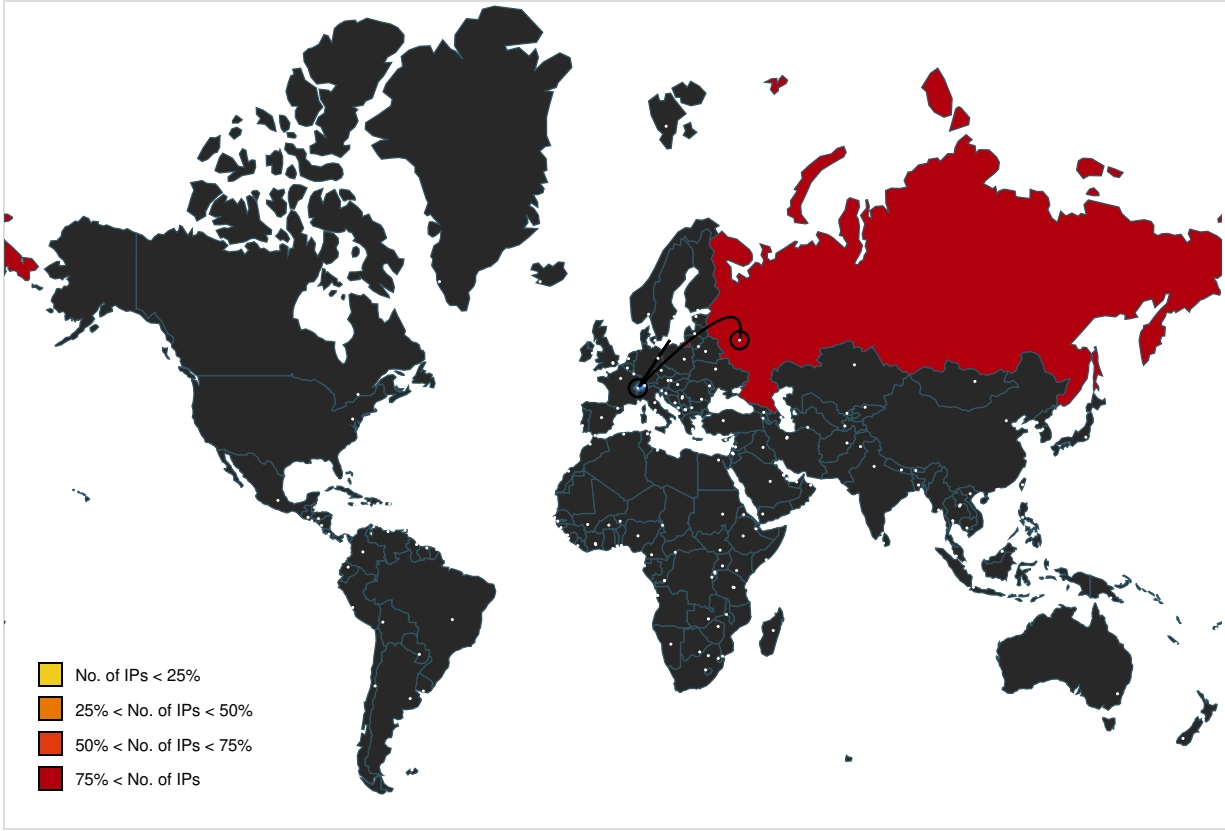
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://62.173.142.51/drew/kjSOZcm1saisXVulw/nMJdjuoxI5rY/D8rf0rwxZvy/xTo4u6qyfG2cqh/DrEm9eSMLtL3Mt_2BWc8v/UHxdAMkcyeaROQd9/EwiLplzlm9gCiDQ/KqEVG_2BN1u2apPrXD/iYwyB9P6y/3dh1O1SBALUj6nSMRJfH/HHlM5d4xQO9d95rkA_2/Bt59zcQMsfJpOgJC8GeSrH/5REGnF8guLwya/xQ1cfd2Y/w3tCRH4bjXIzu_2B_2F_2B5/MmfV_2FK_2/B5ux_2BgxJ6omqMfT/iSBh1mrWB9_2/BRaJgBOq4gEVdF7OIVd_2B/4.jlk	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://62.173.142.51/	server.exe, 00000000.00000002.580573765.0000000000706000.00000004.00000020.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://62.173	server.exe, 00000000.00000002.580755093.000000000281C000.00000004.00000010.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low
http://62.173.142.51/drew/kjSOZcm1saisXVulw/nMJdjuoxI5rY/D8rf0rwxZvy/xTo4u6qyfG2cqh/DrEm9eSMLtL3Mt_2	server.exe, 00000000.00000002.580573765.0000000000706000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	826308
Start date and time:	2023-03-14 15:59:46 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 57s
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:	5
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: 31.5% (good quality ratio 31.5%) • Quality average: 89% • Quality standard deviation: 15.4%

HCA Information:	• Successful, ratio: 90% • 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, WMIADAP.exe, conhost.exe, WmiPrvSE.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.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):	6.482937257572218
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:	192000
MD5:	8f092511c91bfc1f2516e420739a7967
SHA1:	dc67d8f55a6591d16c2709ea65ad143e3a216ec0
SHA256:	9261b47b4fd67523f7afe640e55ccb95ec8b154b5dfa34a8564986ac3e97fe1a
SHA512:	500fa61eec6d02ed95e8a36ffe7160cb1833cd605e3c994d2e1cf09fb7bfd420b1ec3d8f296f863f309fb558afdd77253f5c541dbff1053cc5fbe14df598a154
SSDEEP:	1536:FiqBYFyzXY04aevCQ6V4PLi5jYhsQUFYXxOT6jKBTfjMMTxYjlLmN1j+s8OyWYYE:FfwGezi5jYzTjYMMTxuLmz+scqt7
TLSH:	9A142A0392B07D54F6318A32BE3ECAE9B62FFA514F29776622186E1F05B1071CD62717
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U....j...j...j..~.\..j..~.i..j..~.].Hj....d..j...j..bj..~.X..j..~.m..j..~.j..j..Rich.j.....PE..L....8.b.....

File Icon

Icon Hash:	70d2eeeacacaeadd

Static PE Info

General

Entrypoint:	0x4030a3
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x62AC38B0 [Fri Jun 17 08:17:52 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:	479608e06cc12a8fdc6e43a7370e252b

Entrypoint Preview

Instruction
call 00007F2244AEFFEEh
jmp 00007F2244AED78Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
xor ecx, ecx
cmp eax, dword ptr [0040D008h+ecx*8]
je 00007F2244AED915h
inc ecx
cmp ecx, 2Dh
jc 00007F2244AED8F3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007F2244AED910h
push 0000000Dh
pop eax
pop ebp
ret
mov eax, dword ptr [0040D00Ch+ecx*8]
pop ebp

Instruction
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
pop ebp
ret
call 00007F2244AEFC65h
test eax, eax
jne 00007F2244AED908h
mov eax, 0040D170h
ret
add eax, 08h
ret
call 00007F2244AEFC52h
test eax, eax
jne 00007F2244AED908h
mov eax, 0040D174h
ret
add eax, 0Ch
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
call 00007F2244AED8E7h
mov ecx, dword ptr [ebp+08h]
push ecx
mov dword ptr [eax], ecx
call 00007F2244AED887h
pop ecx
mov esi, eax
call 00007F2244AED8C1h
mov dword ptr [eax], esi
pop esi
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
mov ecx, dword ptr [ebp+08h]
test ecx, ecx
je 00007F2244AED91Dh
push FFFFFFE0h
xor edx, edx
pop eax
div ecx
cmp eax, dword ptr [ebp+0Ch]
jnc 00007F2244AED911h
call 00007F2244AED89Fh
mov dword ptr [eax], 0000000Ch
xor eax, eax
pop ebp
ret
imul ecx, dword ptr [ebp+0Ch]
push esi

Instruction
mov esi, ecx
test esi, esi
jne 00007F2244AED903h

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	0xb73c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9e000	0x10710	.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	0x2c20	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1ac	.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	0xb0dc	0xb200	False	0.5144838483146067	data	6.004854081582009	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xd000	0x9058c	0x13000	False	0.9473555715460527	data	7.85866639754507	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x9e000	0x10710	0x10800	False	0.29835464015151514	data	3.787774889182005	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xac948	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xaca90	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xacbc0	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0xaccb0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x9e6d0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0x9e6d0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0x9e6d0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0x9ef78	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0x9ef78	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway

Name	RVA	Size	Type	Language	Country
RT_ICON	0x9ef78	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa0048	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Sami Lappish	Finland
RT_ICON	0xa0048	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Sami Lappish	Norway
RT_ICON	0xa0048	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Sami Lappish	Sweden
RT_ICON	0xa0ef0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Sami Lappish	Finland
RT_ICON	0xa0ef0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Sami Lappish	Norway
RT_ICON	0xa0ef0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Sami Lappish	Sweden
RT_ICON	0xa1798	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Sami Lappish	Finland
RT_ICON	0xa1798	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Sami Lappish	Norway
RT_ICON	0xa1798	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Sami Lappish	Sweden
RT_ICON	0xa1e60	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Sami Lappish	Finland
RT_ICON	0xa1e60	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Sami Lappish	Norway
RT_ICON	0xa1e60	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Sami Lappish	Sweden
RT_ICON	0xa23c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Sami Lappish	Finland
RT_ICON	0xa23c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Sami Lappish	Norway
RT_ICON	0xa23c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Sami Lappish	Sweden
RT_ICON	0xa4970	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Sami Lappish	Finland
RT_ICON	0xa4970	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Sami Lappish	Norway
RT_ICON	0xa4970	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Sami Lappish	Sweden
RT_ICON	0xa5a18	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Sami Lappish	Finland
RT_ICON	0xa5a18	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Sami Lappish	Norway
RT_ICON	0xa5a18	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Sami Lappish	Sweden
RT_ICON	0xa63a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Sami Lappish	Finland
RT_ICON	0xa63a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Sami Lappish	Norway
RT_ICON	0xa63a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Sami Lappish	Sweden
RT_ICON	0xa6880	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa6880	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa6880	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa7728	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa7728	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa7728	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa7df0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa7df0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa7df0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa8358	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa8358	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa8358	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xaa900	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xaa900	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xaa900	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xab9a8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xab9a8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xab9a8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xac330	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xac330	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xac330	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Sweden
RT_STRING	0xadfe0	0x3be	data	Sami Lappish	Finland
RT_STRING	0xadfe0	0x3be	data	Sami Lappish	Norway
RT_STRING	0xadfe0	0x3be	data	Sami Lappish	Sweden
RT_STRING	0xae3a0	0x36a	data	Sami Lappish	Finland
RT_STRING	0xae3a0	0x36a	data	Sami Lappish	Norway
RT_STRING	0xae3a0	0x36a	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xac8a8	0x90	data	Sami Lappish	Finland
RT_ACCELERATOR	0xac8a8	0x90	data	Sami Lappish	Norway
RT_ACCELERATOR	0xac8a8	0x90	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xac800	0xa8	data	Sami Lappish	Finland
RT_ACCELERATOR	0xac800	0xa8	data	Sami Lappish	Norway
RT_ACCELERATOR	0xac800	0xa8	data	Sami Lappish	Sweden
RT_GROUP_CURSOR	0xaca78	0x14	data		
RT_GROUP_CURSOR	0xadd58	0x30	data		
RT_GROUP_ICON	0xa0020	0x22	data	Sami Lappish	Finland
RT_GROUP_ICON	0xa0020	0x22	data	Sami Lappish	Norway
RT_GROUP_ICON	0xa0020	0x22	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xa6808	0x76	data	Sami Lappish	Finland
RT_GROUP_ICON	0xa6808	0x76	data	Sami Lappish	Norway
RT_GROUP_ICON	0xa6808	0x76	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xac798	0x68	data	Sami Lappish	Finland
RT_GROUP_ICON	0xac798	0x68	data	Sami Lappish	Norway
RT_GROUP_ICON	0xac798	0x68	data	Sami Lappish	Sweden
RT_VERSION	0xadd88	0x254	data		
None	0xac938	0xa	data	Sami Lappish	Finland
None	0xac938	0xa	data	Sami Lappish	Norway
None	0xac938	0xa	data	Sami Lappish	Sweden

Imports

DLL	Import

DLL	Import
KERNEL32.dll	lstrcmpA, FindFirstFileW, EnumCalendarInfoA, _llseek, WritePrivateProfileSectionA, GlobalLock, InterlockedCompareExchange, SleepEx, GetModuleHandleW, EnumCalendarInfoExW, EnumTimeFormatsW, WriteFileGather, EnumResourceTypesA, GlobalAlloc, GetSystemDirectoryW, AddRefActCtx, GetSystemWindowsDirectoryA, LeaveCriticalSection, GetConsoleAliasW, GetFileAttributesW, SetDefaultCommConfigA, GetCPInfoExW, SetLastError, GetProcAddress, CopyFileA, GetFirmwareEnvironmentVariableW, LoadLibraryA, OpenWaitableTimerW, FindFirstVolumeMountPointW, GetExitCodeThread, AddAtomW, CreateEventW, AddAtomA, FindNextFileW, GetShortPathNameW, SetCalendarInfoA, ReadConsoleInputW, LocalSize, CopyFileExA, RaiseException, PulseEvent, GetLastError, MoveFileA, DeleteFileA, HeapReAlloc, GetCommandLineA, HeapSetInformation, GetStartupInfoW, HeapAlloc, EnterCriticalSection, DecodePointer, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, EncodePointer, TerminateProcess, GetCurrentProcess, HeapCreate, HeapFree, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameW, GetModuleFileNameA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, SetHandleCount, InitializeCriticalSectionAndSpinCount, GetFileType, DeleteCriticalSection, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, InterlockedDecrement, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, Sleep, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, RtlUnwind, LoadLibraryW, GetConsoleCP, GetConsoleMode, FlushFileBuffers, LCMapStringW, MultiByteToWideChar, GetStringTypeW, SetFilePointer, IsProcessorFeaturePresent, HeapSize, CloseHandle, WriteConsoleW, SetStdHandle, CreateFileW
USER32.dll	LoadMenuW
ADVAPI32.dll	LookupAccountSidW

Possible Origin

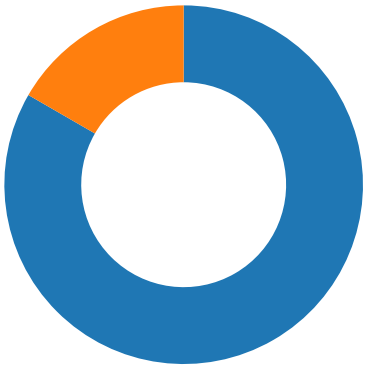
Language of compilation system	Country where language is spoken	Map
Sami Lappish	Finland	
Sami Lappish	Norway	
Sami Lappish	Sweden	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.562.173.142.51 49680802033203 03/14/23-16:02:33.550566	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49680	80	192.168.2.5	62.173.142.51

Network Port Distribution



Total Packets: 6

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 14, 2023 16:02:33.490955114 CET	49680	80	192.168.2.5	62.173.142.51
Mar 14, 2023 16:02:33.550028086 CET	80	49680	62.173.142.51	192.168.2.5
Mar 14, 2023 16:02:33.550132990 CET	49680	80	192.168.2.5	62.173.142.51
Mar 14, 2023 16:02:33.550565958 CET	49680	80	192.168.2.5	62.173.142.51
Mar 14, 2023 16:02:33.609353065 CET	80	49680	62.173.142.51	192.168.2.5
Mar 14, 2023 16:02:33.609383106 CET	80	49680	62.173.142.51	192.168.2.5
Mar 14, 2023 16:02:33.609524965 CET	49680	80	192.168.2.5	62.173.142.51
Mar 14, 2023 16:02:33.612766027 CET	49680	80	192.168.2.5	62.173.142.51
Mar 14, 2023 16:02:33.671506882 CET	80	49680	62.173.142.51	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 14, 2023 16:01:13.337074041 CET	61325	53	192.168.2.5	8.8.8.8
Mar 14, 2023 16:01:13.363226891 CET	53	61325	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 14, 2023 16:01:13.337074041 CET	192.168.2.5	8.8.8.8	0xce38	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 14, 2023 16:01:13.363226891 CET	8.8.8.8	192.168.2.5	0xce38	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 62.173.142.51

Statistics

No statistics

System Behavior

Analysis Process: server.exe PID: **5540**, Parent PID: **3324**

General

Target ID:	0
Start time:	16:00:49
Start date:	14/03/2023
Path:	C:\Users\user\Desktop\server.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\server.exe
Imagebase:	0x400000

File size:	192000 bytes
MD5 hash:	8F092511C91BFC1F2516E420739A7967
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: 00000000.00000003.494639050.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494639050.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494639050.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494532027.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494532027.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494532027.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.580772569.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.580772569.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.580772569.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494557591.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494557591.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494557591.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494507047.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494507047.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494507047.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494595207.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494595207.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494595207.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494478374.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494478374.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494478374.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.580453253.0000000000540000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.580553464.00000000006A8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494674831.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494674831.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494674831.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.494622294.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.494622294.0000000002C68000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.494622294.0000000002C68000.00000004.00000020.00020000.00000000.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