ID: 825996
Sample Name: server.exe
Cookbook: default.jbs
Time: 08:23:06
Date: 14/03/2023
Version: 37.0.0 Beryl

Table of Contents

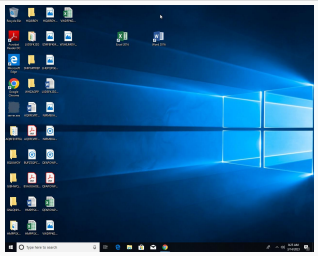
Windows Analysis Report

server.exe

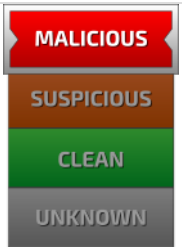
Overview

General Information

Sample Name:	server.exe
Analysis ID:	825996
MD5:	bfe5c79a11ef4…
SHA1:	bd04d26776c7…
SHA256:	881d60034e97…
Tags:	agenziaentrate exe gozi isfb ITA mef mise ursnif
Infos:	



Detection



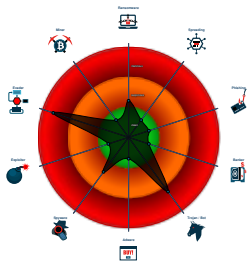
Ursnif

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

Signatures

- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- 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…
- Creates a DirectInput object (often f…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- server.exe (PID: 6020 cmdline: C:\Users\user\Desktop\server.exe MD5: BFE5C79A11EF437D401FE8A27EA49372)
- **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
00000000.00000002.509856527.0000000000850000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x58a1:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.509728577.0000000000780000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000003.439407520.0000000002F18000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.439407520.0000000002F18000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.439407520.0000000002F18000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$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\

Click to see the 27 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

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)

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

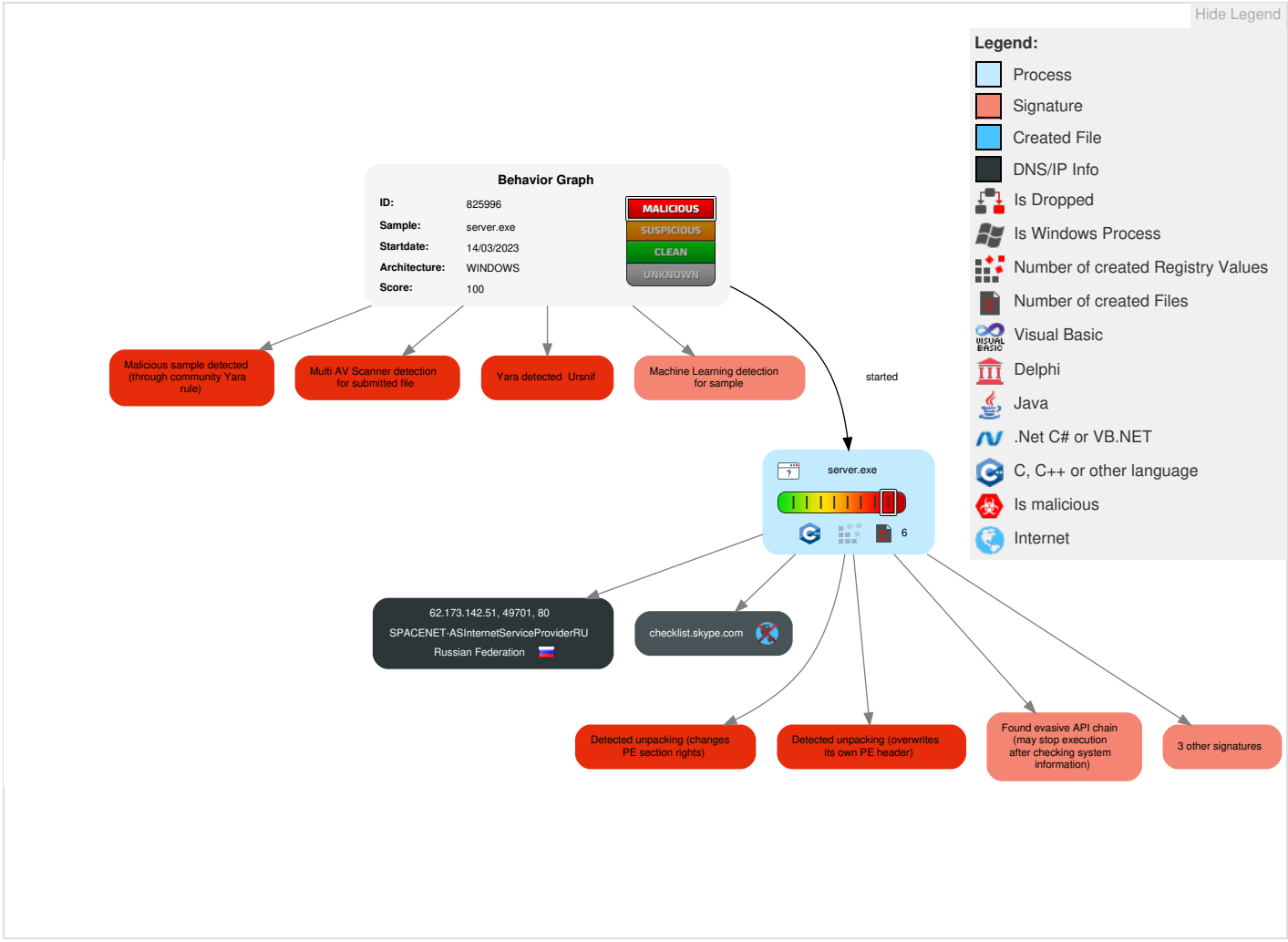
Remote Access Functionality

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

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
server.exe	38%	ReversingLabs	Win32.Trojan.Generic	
server.exe	51%	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.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.server.exe.7e0000.2.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://62.173.142.51/	0%	Avira URL Cloud	safe	
http://62.173.142.51/drew/9JLLLQ08ZT/3nAR5UipYIcJ6YCNU/DQSgo3cwsXXD/wvZ5vmAsFoS/eN07eLMp7RXTwB/STvLb_2BVZ4b1fMQvftqC/DrhbQbfPiZSBlmnh/Q60mymncnsD1BSl/lgW04WzkBwMabSScvE/3MDL0Eyu0/chVZbMtmkjfLI4ISTEnD/sLlQp4wto2w2tJ4sMhW/deWpiBQ03TPTGzGU4_2FTK/eoq2qHiaYlnL2/Y44FiYqv/mKJo7GKlTdrY4JvUjnEzoh2/JtdyUM2ECt/vn.jlk	0%	Avira URL Cloud	safe	
http://62.173.142.51/b	0%	Avira URL Cloud	safe	
http://62.173.142.51/drew/9JLLLQ08ZT/3nAR5UipYIcJ6YCNU/DQSgo3cwsXXD/wvZ5vmAsFoS/eN07eLMp7RXTwB/STvLb	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
windowsupdatebg.s.llnwi.net	95.140.230.192	true	false		unknown
checklist.skype.com	unknown	unknown	false		high

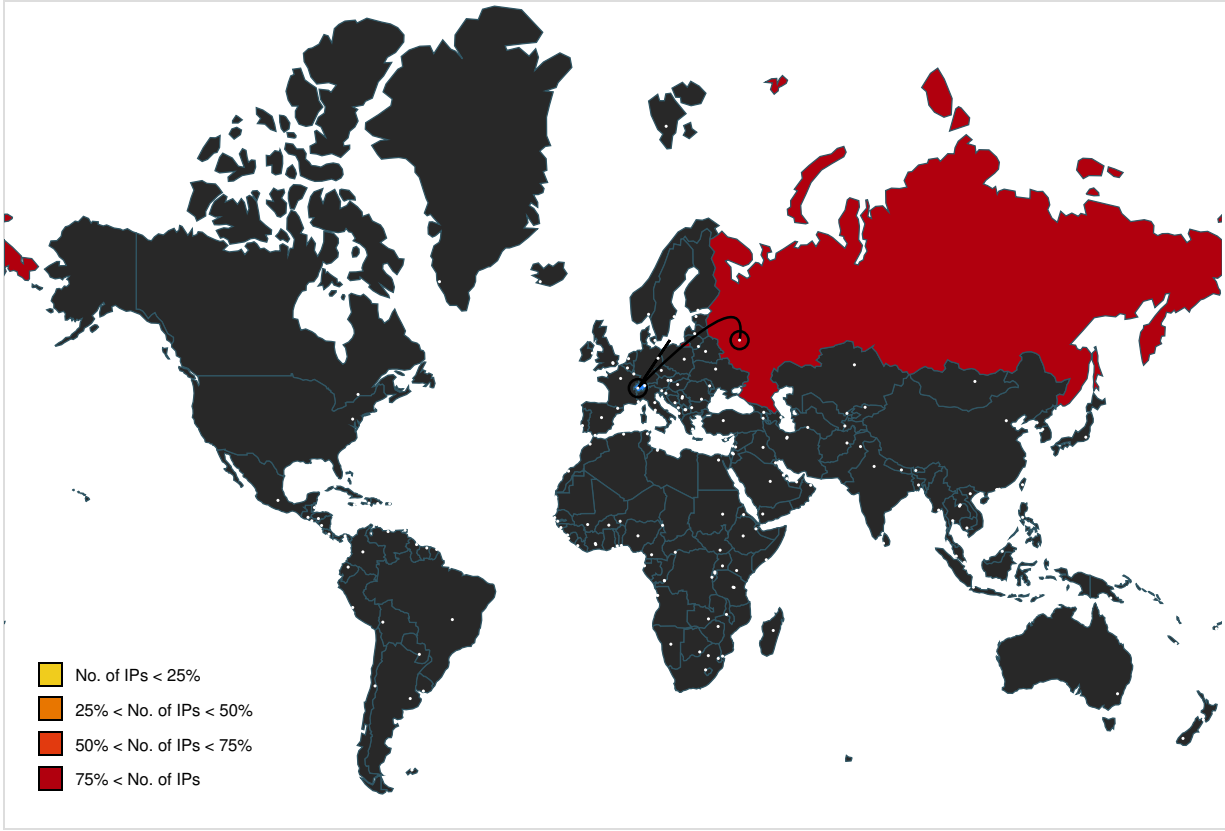
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://62.173.142.51/drew/9JLLLQ08ZT/3nAR5UipYIcJ6YCNU/DQSgo3cwsXXD/wvZ5vmAsFoS/eN07eLMp7RXTwB/STvLb_2BVZ4b1fMQvftqC/DrhbQbfPiZSBlmnh/Q60mymncnsD1BSl/lgW04WzkBwMabSScvE/3MDL0Eyu0/chVZbMtmkjfLI4ISTEnD/sLlQp4wto2w2tJ4sMhW/deWpiBQ03TPTGzGU4_2FTK/eoq2qHiaYlnL2/Y44FiYqv/mKJo7GKlTdrY4JvUjnEzoh2/JtdyUM2ECt/vn.jlk	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://62.173.142.51/b	server.exe, 00000000.00000002.509818085.0000000000830000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.173.142.51/	server.exe, 00000000.00000002.509882695.0000000000863000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://checklist.skype.com/drew/libExsiR_2B8yxsG/gzT0k6OLSRpq780/hHFpS0TQeiCZoSZxmo/_2BfNC9Bm/rlL_2B	server.exe, 00000000.00000002.509882695.0000000000863000.00000004.00000020.00020000.00000000.sdmp	false		high
http://62.173	server.exe, 00000000.00000002.510020655.00000000023CC000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://62.173.142.51/drew/9JLLLQ08ZT/3nAR5UipYIcJ6YCNU/DQSgo3cwsXXD/wvZ5vmAsFoS/eN07eLMp7RXTwB/STvLb	server.exe, 00000000.00000002.509882695.00000000008A6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	825996
Start date and time:	2023-03-14 08:23:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 45s
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:	13
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: 18.4% (good quality ratio 17.6%) • Quality average: 81.1% • Quality standard deviation: 27.8%

HCA Information:	• Successful, ratio: 100% • 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, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 209.197.3.8, 93.184.221.240
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, wu.ec.azureedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, www-www.bing.com.trafficmanager.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net, dual-a-0001.dc-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net
- 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):	6.821157222424382

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:	239104
MD5:	bfe5c79a11ef437d401fe8a27ea49372
SHA1:	bd04d26776c766934f0acd2885cf97168dc5bbfb
SHA256:	881d60034e97cfa4e36b8da907e5d2e130c9f19abdd386990ee5a9cdce91d117
SHA512:	4b803dd0a1f8c378d4e61f753aa84a690908dcd2de8289e331f4b7cbbc28480883f7b26f272dfc0e109ef133a59642f2221981caf4dcaae6412a2439a2e38fb9
SSDEEP:	6144:ilOuqy8KhQd+1x8toQRwwzsjqxn2Sc4gKO:iLTydhQdjtoR8sjqxn2ScKO
TLSH:	CA349E137391A871E6324A31BE1BC2F5661EFCA44F5967EB23946A2F0D752E1CE31342
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....aBL...L...L...#...\...#.../...E...G...L...:...#...a...#...M...#...M...RichL.....PE..L.....b.....

File Icon

Icon Hash:	9a82325a89a28ab2

Static PE Info

General

Entrypoint:	0x409761
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:	0x620D9091 [Thu Feb 17 00:02:25 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:	ae274c29ca15928cb1e23f2e712ba155

Entrypoint Preview

Instruction
call 00007F46FCF0236Eh
jmp 00007F46FCEFBD8Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
test eax, eax
je 00007F46FCEFBF14h
sub eax, 08h
cmp dword ptr [eax], 0000DDDDh
jne 00007F46FCEFBF09h
push eax
call 00007F46FCEFB527h
pop ecx
pop ebp
ret
mov edi, edi

Instruction
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007F46FCEFBF65h
call 00007F46FCEFEEDDh
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [0042D340h]
je 00007F46FCEFBF14h
mov ecx, dword ptr [0042D0F8h]
test dword ptr [eax+70h], ecx
jne 00007F46FCEFBF09h
call 00007F46FCF02D48h
mov dword ptr [esi], eax
mov eax, dword ptr [esi+04h]
cmp eax, dword ptr [0042D000h]
je 00007F46FCEFBF18h
mov eax, dword ptr [esi+08h]
mov ecx, dword ptr [0042D0F8h]
test dword ptr [eax+70h], ecx
jne 00007F46FCEFBF0Ah
call 00007F46FCF025A7h
mov dword ptr [esi+04h], eax
mov eax, dword ptr [esi+08h]
test byte ptr [eax+70h], 00000002h
jne 00007F46FCEFBF16h
or dword ptr [eax+70h], 02h
mov byte ptr [esi+0Ch], 00000001h
jmp 00007F46FCEFBF0Ch
mov ecx, dword ptr [eax]
mov dword ptr [esi], ecx
mov eax, dword ptr [eax+04h]
mov dword ptr [esi+04h], eax
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 10h
mov eax, dword ptr [0042C908h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
mov edx, dword ptr [ebp+18h]
push ebx

Rich Headers

Programming Language:	• [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [C++] VS2010 build 30319 • [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	0x18f6c	0x78	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xab000	0xdd08	.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	0x4320	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.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	0x18a14	0x18c00	False	0.5078519570707071	data	6.313918932739284	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x90e88	0x13800	False	0.9314778645833334	data	7.82921848401168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xab000	0xdd08	0xde00	False	0.4086782094594595	data	4.407077801593062	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xb6f48	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xb7090	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xb71c0	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0xb72b0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0xab5e0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xab5e0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xab5e0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xabe88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xabe88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xabe88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xacf58	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xacf58	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xacf58	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden

Name	RVA	Size	Type	Language	Country
RT_ICON	0xad800	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xad800	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xad800	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xafda8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xafda8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xafda8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb0e80	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xb0e80	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xb0e80	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xb1d28	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xb1d28	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xb1d28	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xb23f0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xb23f0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xb23f0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xb2958	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb2958	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb2958	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb4f00	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb4f00	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb4f00	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb5fa8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb5fa8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb5fa8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb6930	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb6930	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb6930	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Sweden
RT_STRING	0xb85d8	0x3be	data	Sami Lappish	Finland
RT_STRING	0xb85d8	0x3be	data	Sami Lappish	Norway
RT_STRING	0xb85d8	0x3be	data	Sami Lappish	Sweden
RT_STRING	0xb8998	0x36a	data	Sami Lappish	Finland
RT_STRING	0xb8998	0x36a	data	Sami Lappish	Norway
RT_STRING	0xb8998	0x36a	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xb6ea8	0x90	data	Sami Lappish	Finland
RT_ACCELERATOR	0xb6ea8	0x90	data	Sami Lappish	Norway
RT_ACCELERATOR	0xb6ea8	0x90	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xb6e00	0xa8	data	Sami Lappish	Finland
RT_ACCELERATOR	0xb6e00	0xa8	data	Sami Lappish	Norway
RT_ACCELERATOR	0xb6e00	0xa8	data	Sami Lappish	Sweden
RT_GROUP_CURSOR	0xb7078	0x14	data		
RT_GROUP_CURSOR	0xb8358	0x30	data		

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0xb0e50	0x30	data	Sami Lappish	Finland
RT_GROUP_ICON	0xb0e50	0x30	data	Sami Lappish	Norway
RT_GROUP_ICON	0xb0e50	0x30	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xacf30	0x22	data	Sami Lappish	Finland
RT_GROUP_ICON	0xacf30	0x22	data	Sami Lappish	Norway
RT_GROUP_ICON	0xacf30	0x22	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xb6d98	0x68	data	Sami Lappish	Finland
RT_GROUP_ICON	0xb6d98	0x68	data	Sami Lappish	Norway
RT_GROUP_ICON	0xb6d98	0x68	data	Sami Lappish	Sweden
RT_VERSION	0xb8388	0x24c	data		
None	0xb6f38	0xa	data	Sami Lappish	Finland
None	0xb6f38	0xa	data	Sami Lappish	Norway
None	0xb6f38	0xa	data	Sami Lappish	Sweden

Imports

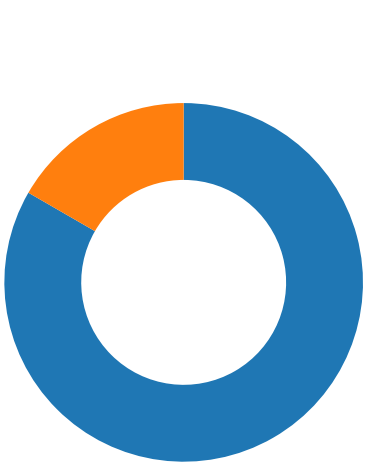
DLL	Import
KERNEL32.dll	PulseEvent, ReadConsoleInputW, GetFirmwareEnvironmentVariableW, GetCPInfoExW, CreateEventW, CopyFileExA, GetProcAddress, GlobalAlloc, SetDefaultCommConfigA, OpenWaitableTimerW, GetFileAttributesW, EnumResourceTypesW, WriteFileGather, GetModuleHandleW, InterlockedCompareExchange, UnhandledExceptionFilter, LocalFlags, GlobalLock, GetConsoleAliasW, WritePrivateProfileSectionA, FindFirstVolumeMountPointA, SetLastError, SleepEx, AddAtomA, lstrcmpA, SetCalendarInfoA, GetSystemWindowsDirectoryA, EnumTimeFormatsW, GetSystemDirectoryW, AddAtomW, GetExitCodeThread, _llseek, FindNextFileW, CopyFileA, GetShortPathNameW, EnumCalendarInfoA, EnumCalendarInfoExA, AddRefActCtx, SetStdHandle, WriteConsoleW, GetCurrentThreadId, LoadLibraryA, CloseHandle, SetFilePointer, ReadFile, FlushFileBuffers, InterlockedIncrement, InterlockedDecrement, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, EncodePointer, DecodePointer, GetLastError, HeapFree, RtlUnwind, RaiseException, HeapReAlloc, HeapAlloc, MoveFileA, DeleteFileA, GetCommandLineA, HeapSetInformation, GetStartupInfoW, WideCharToMultiByte, LCMapStringW, MultiByteToWideChar, GetCPInfo, IsProcessorFeaturePresent, HeapCreate, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameW, SetUnhandledExceptionFilter, IsDebuggerPresent, TerminateProcess, GetCurrentProcess, GetModuleFileNameA, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, InitializeCriticalSectionAndSpinCount, GetFileType, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetACP, GetOEMCP, IsValidCodePage, GetStringTypeW, GetLocaleInfoW, HeapSize, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, LoadLibraryW, GetConsoleCP, GetConsoleMode, CreateFileW
USER32.dll	LoadMenuW
ADVAPI32.dll	LookupAccountSidW
SHELL32.dll	FindExecutableA
ole32.dll	CoGetInstanceFromFile

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 14, 2023 08:25:50.375926018 CET	49701	80	192.168.2.3	62.173.142.51
Mar 14, 2023 08:25:50.436150074 CET	80	49701	62.173.142.51	192.168.2.3
Mar 14, 2023 08:25:50.436259031 CET	49701	80	192.168.2.3	62.173.142.51
Mar 14, 2023 08:25:50.436628103 CET	49701	80	192.168.2.3	62.173.142.51
Mar 14, 2023 08:25:50.495964050 CET	80	49701	62.173.142.51	192.168.2.3
Mar 14, 2023 08:25:50.496022940 CET	80	49701	62.173.142.51	192.168.2.3
Mar 14, 2023 08:25:50.496108055 CET	49701	80	192.168.2.3	62.173.142.51
Mar 14, 2023 08:25:50.498536110 CET	49701	80	192.168.2.3	62.173.142.51
Mar 14, 2023 08:25:50.557815075 CET	80	49701	62.173.142.51	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 14, 2023 08:24:30.206993103 CET	62704	53	192.168.2.3	8.8.8.8
Mar 14, 2023 08:24:30.228854895 CET	53	62704	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 14, 2023 08:24:30.206993103 CET	192.168.2.3	8.8.8.8	0x2dc2	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 08:23:52.986346006 CET	8.8.8.8	192.168.2.3	0x15a2	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)	false
Mar 14, 2023 08:24:30.228854895 CET	8.8.8.8	192.168.2.3	0x2dc2	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 62.173.142.51

Chrome Debug Log

Statistics

No statistics

System Behavior

Analysis Process: server.exe PID: 6020, Parent PID: 3452

General

Target ID:	0
Start time:	08:23:58
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:	239104 bytes
MD5 hash:	BFE5C79A11EF437D401FE8A27EA49372
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.509856527.0000000000850000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.509728577.0000000000780000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439407520.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.439407520.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.439407520.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439271373.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.439271373.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.439271373.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439423736.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.439423736.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.439423736.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439453495.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.439453495.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.439453495.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.510107149.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.510107149.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439387430.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.439387430.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.439387430.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.510107149.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439306585.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.439306585.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.439306585.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439442593.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.439442593.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.439442593.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439341989.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.439341989.0000000002F18000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.439341989.0000000002F18000.00000004.00000020.00020000.00000000.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