ID: 830522
Sample Name: Server.exe
Cookbook: default.jbs
Time: 13:12:45
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

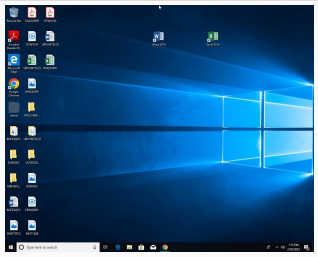
Windows Analysis Report

Server.exe

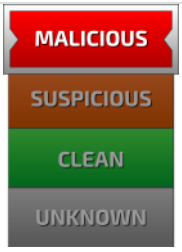
Overview

General Information

Sample Name:	Server.exe
Analysis ID:	830522
MD5:	9565b4a15a85…
SHA1:	0954c5387395…
SHA256:	3aa75da27735…
Tags:	250255 7715 exe geo Gozi ITA Ursnif
Infos:	



Detection



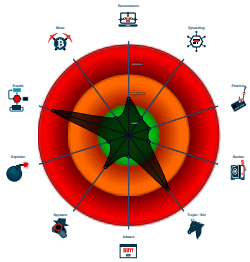
Ursnif

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- Server.exe (PID: 5744 cmdline: C:\Users\user\Desktop\Server.exe MD5: 9565B4A15A8593EA3EC1F3C9D0A2E11A)
- **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/ySpD96hQxlGzGgDApS0E
54E54SLEBTqihX3FWN2//mDaDIJuoFz7lt0whvCg/8gXPBf/s2nkXoRwyyqXguvwDcw9IZEu1NT1qqIwpXL9DGlddMvwfXTGOLIkQX35RsJJDpP1V5Mcgc+c1nBRPKqGQz+NUtKDBiyp0RXMK3jDdMGWvimLl80kvMkvSd8fQXtWRcZ7D
CuQwrQxkXo=",
  "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
00000000.00000002.513518394.00000000004E6000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x5a70:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.513718671.0000000001FC0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000002.513908853.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000002.513908853.0000000002CA8000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000002.513908853.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$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\

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: 192.168.2.6 - Destination IP: 193.233.175.113

Timestamp:	192.168.2.6193.233.175.11349705802033204 03/20/23-13:15:36.320401
SID:	2033204

Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.6 - Destination IP: 62.173.142.81	−
Timestamp:	192.168.2.662.173.142.8149704802033203 03/20/23-13:15:16.126464
SID:	2033203
Source Port:	49704
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.6 - Destination IP: 62.173.142.81	−
Timestamp:	192.168.2.662.173.142.8149704802033204 03/20/23-13:15:16.126464
SID:	2033204
Source Port:	49704
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

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

Anti Debugging

Found API chain indicative of debugger detection

Stealing of Sensitive Information

Yara detected Ursnif

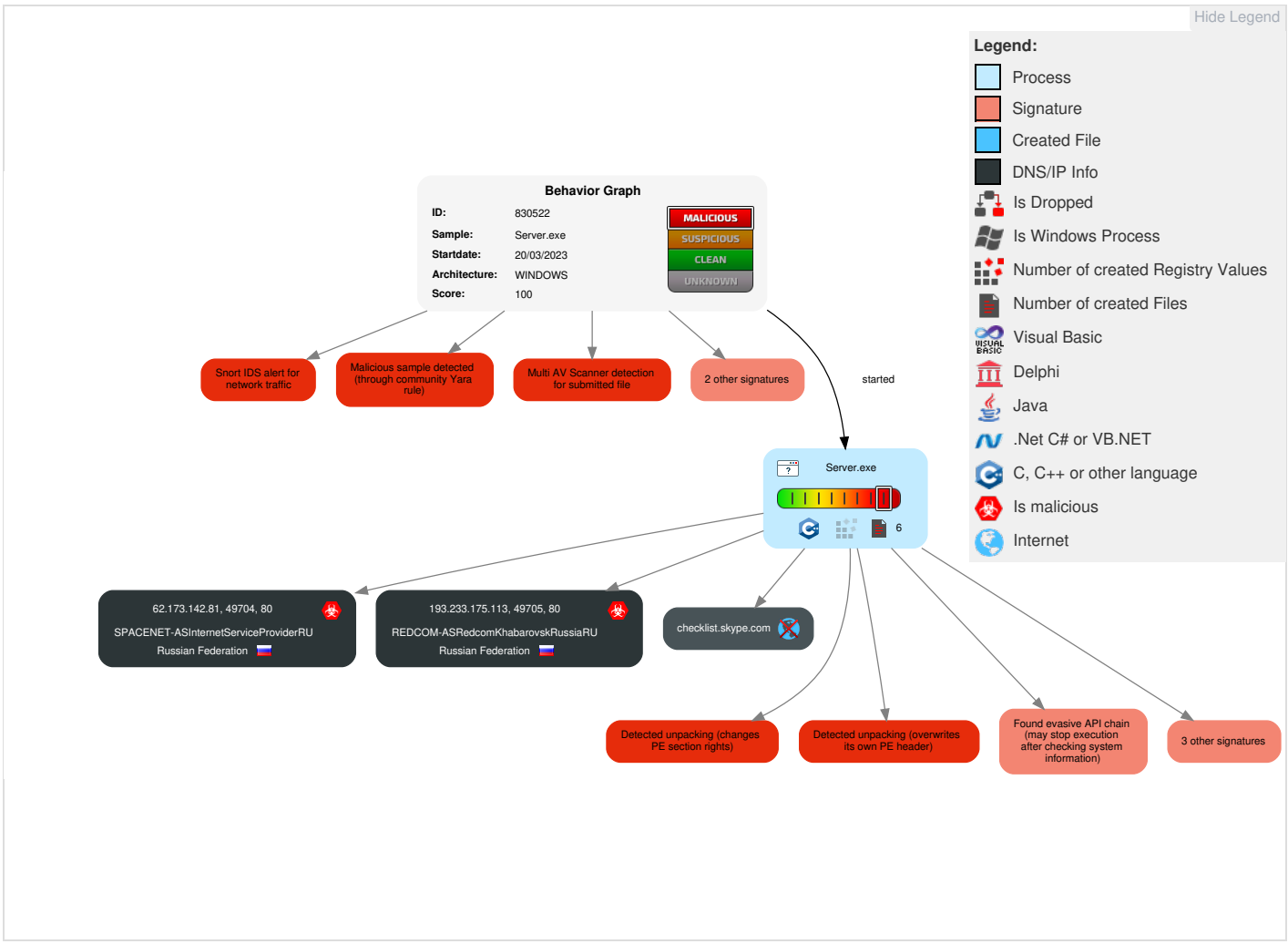
Remote Access Functionality

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	1 1 Archive Collected Data	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 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	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 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

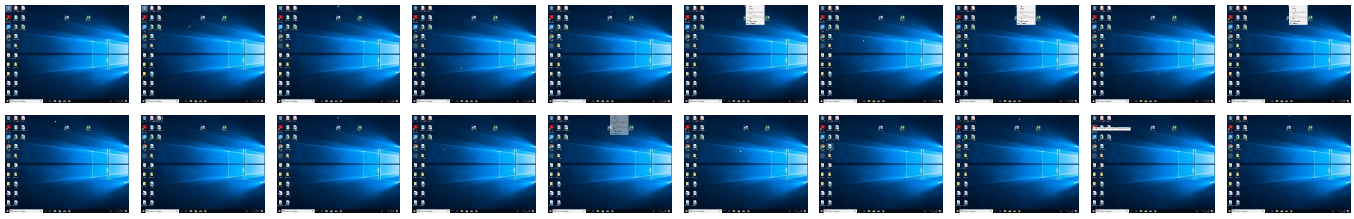
Behavior Graph



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	36%	ReversingLabs	Win32.Trojan.Generic	
Server.exe	46%	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.2020000.2.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://193.23	0%	Avira URL Cloud	safe	
http://62.173.142.81/drew/vtZ_2FDli/MRLim5q_2FPOOIVwJV5p/mDG55l02bkwr36hqtHV/_2BXyU_2BkyUgVl9WIyeMc/2k07Y9nJ9nLtT/PcL77Drj/unLXMitiTeAgURShweMUOiB/jO6Gh6u4qj/R0YL8nr8_2Fe_2F8S/NmYC2zbFo_2F/_2F9OVp7R5L/glgHLP7bYaSidB/FZsufB1rfZCbhP2GWCC1X/tQ2Xe4zo9AyYJ7HA/jNvemogj1MfecHx/YKLEAqQON4Cy4b59f3/zq6LmLb43/Vud6lYhHL1LCLqJWQEpj/MZMy2z9wXkXjHl/Y_2BX.jlk	0%	Avira URL Cloud	safe	
http://193.233.175.113/drew/qHKukbBQWu/Xw77sqXTqtrxRWpPD/yl9MR0Y2eNmn/GbsfhYjdl8H/5GaIgAKgHB90sh/aMn4M6bKKJciYELDTreaM/i8dqMbDS0rDZpO_2/F2s0PNMupq8bNg2/sWxA9_2FGI7DvJntWq/sJDzxIUTO/r8bT3UibSNEQXXaTJdFi/yG6uB8JAsWc6GRKrJig/fWv9nw4MT1weBq8HJPcdl7/ZF86bHFVi_2FJ/yinUV20K/IPPC4VuFn7ORSOMnH_2FY6_/2FwmfjECDI/_2B41PRFw9jRfkH5W/0EbKz9E3ebE/0M10.jlk	0%	Avira URL Cloud	safe	
http://193.23	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

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

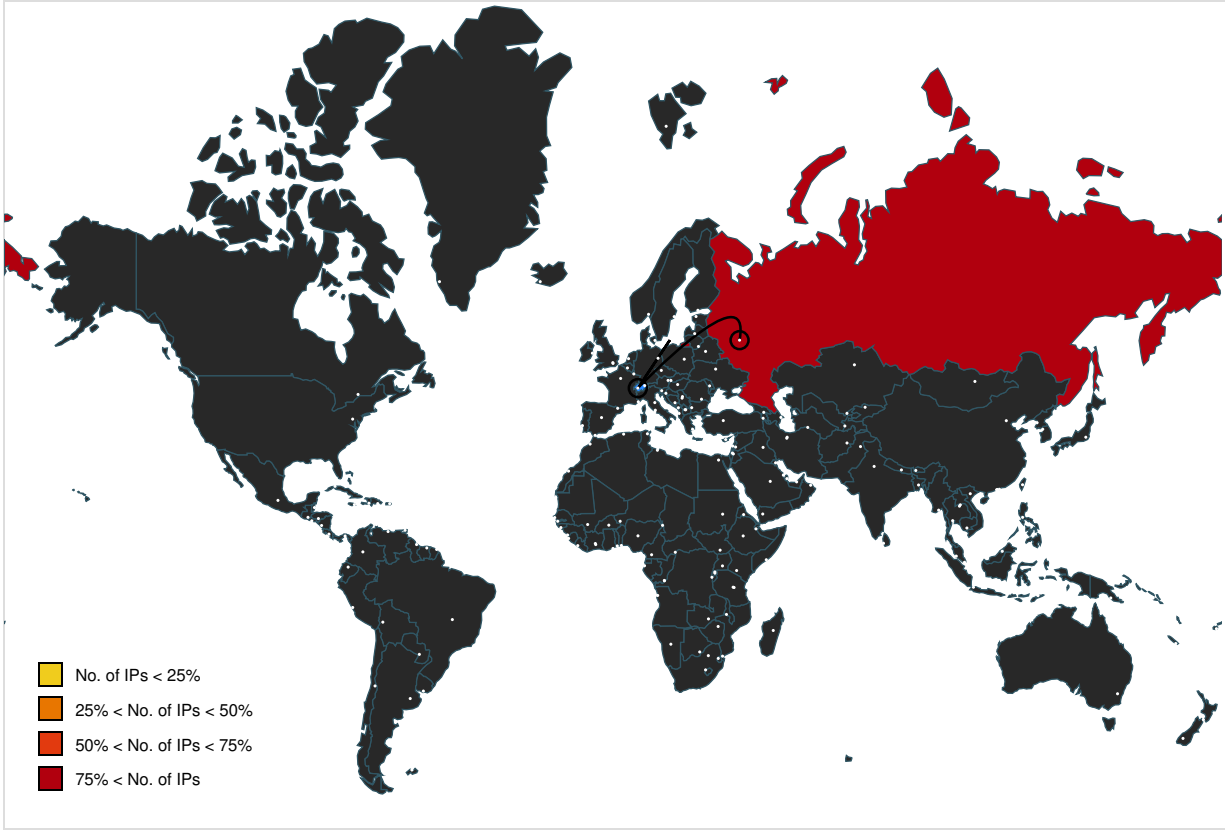
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://62.173.142.81/drew/vtZ_2FDli/MRLim5q_2FPOOIVwJV5p/mDG55l02bkwr36hqtHV/_2BXyU_2BkyUgVl9WIyeMc/2k07Y9nJ9nLtT/PcL77Drj/unLXMitiTeAgURShweMUOiB/jO6Gh6u4qj/R0YL8nr8_2Fe_2F8S/NmYC2zbFo_2F/_2F9OVp7R5L/glgHLP7bYaSidB/FZsufB1rfZCbhP2GWCC1X/tQ2Xe4zo9AyYJ7HA/jNvemogj1MfecHx/YKLEAqQON4Cy4b59f3/zq6LmLb43/Vud6lYhHL1LCLqJWQEpj/MZMy2z9wXkXjHl/Y_2BX.jlk	true	• Avira URL Cloud: safe	unknown
http://193.233.175.113/drew/qHKukbBQWu/Xw77sqXTqtrxRWpPD/yl9MR0Y2eNmn/GbsfhYjdl8H/5GaIgAKgHB90sh/aMn4M6bKKJciYELDTreaM/i8dqMbDS0rDZpO_2/F2s0PNMupq8bNg2/sWxA9_2FGI7DvJntWq/sJDzxIUTO/r8bT3UibSNEQXXaTJdFi/yG6uB8JAsWc6GRKrJig/fWv9nw4MT1weBq8HJPcdl7/ZF86bHFVi_2FJ/yinUV20K/IPPC4VuFn7ORSOMnH_2FY6_/2FwmfjECDI/_2B41PRFw9jRfkH5W/0EbKz9E3ebE/0M10.jlk	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://193.23	Server.exe, 00000000.00000002.513863268.00000000023BC000.00000004.00000010.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • 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
193.233.175.113	unknown	Russian Federation		8749	REDCOM-ASRedcomKhabarovskRussiaRU	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830522
Start date and time:	2023-03-20 13:12:45 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 54s
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@1/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 41.6% (good quality ratio 39.7%) • Quality average: 81.1% • Quality standard deviation: 27.9%
HCA Information:	• Successful, ratio: 98% • 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 domains from analysis (whitelisted): fs.microsoft.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):	6.812179089793973

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:	9565b4a15a8593ea3ec1f3c9d0a2e11a
SHA1:	0954c5387395f0552fa56f5b06b3bb159f0d430b
SHA256:	3aa75da2773573786f07530f5a09b8e0aacd0402fd11e14d8067b5f4607bbd6a
SHA512:	38c39811e09b664c70da24370fdc2cb555d698a1db868ed236d86c767cf5fb8751e8f5f1db667a4d807f6db39f8511b4753cfc59d9c85d0daa60ebef81a6adb8
SSDEEP:	3072:iu7sH/YqGkGehHskiO+hMIPZSyqGr7tA0jtejRXwtig0:psfYq/72jhMIhSyzrh7jte9Oig
TLSH:	16049EC392A07C51E4268A368E2FC2F4770DF891CE59AB66F3186F2F48BC172D562751
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.b.....

File Icon

Icon Hash:	ba824242a5a2a28a

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:	0x62DB63E7 [Sat Jul 23 02:58:47 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:	2bf4bd16bd9a3948cc472dde1e8c8ccd

Entrypoint Preview

Instruction
call 00007F66CD126790h
jmp 00007F66CD123DBEh
mov eax, 0040D008h
ret
mov eax, dword ptr [0049D980h]
push esi
push 00000014h
pop esi
test eax, eax
jne 00007F66CD123F39h
mov eax, 00000200h
jmp 00007F66CD123F38h
cmp eax, esi
jnl 00007F66CD123F39h
mov eax, esi
mov dword ptr [0049D980h], eax
push 00000004h

Instruction
push eax
call 00007F66CD12683Eh
pop ecx
pop ecx
mov dword ptr [0049C960h], eax
test eax, eax
jne 00007F66CD123F50h
push 00000004h
push esi
mov dword ptr [0049D980h], esi
call 00007F66CD126825h
pop ecx
pop ecx
mov dword ptr [0049C960h], eax
test eax, eax
jne 00007F66CD123F37h
push 0000001Ah
pop eax
pop esi
ret
xor edx, edx
mov ecx, 0040D008h
jmp 00007F66CD123F37h
mov eax, dword ptr [0049C960h]
mov dword ptr [edx+eax], ecx
add ecx, 20h
add edx, 04h
cmp ecx, 0040D288h
jl 00007F66CD123F1Ch
push FFFFFFFEh
pop esi
xor edx, edx
mov ecx, 0040D018h
push edi
mov eax, edx
sar eax, 05h
mov eax, dword ptr [0049C860h+eax*4]
mov edi, edx
and edi, 1Fh
shl edi, 06h
mov eax, dword ptr [edi+eax]
cmp eax, FFFFFFFFh
je 00007F66CD123F3Ah
cmp eax, esi
je 00007F66CD123F36h
test eax, eax
jne 00007F66CD123F34h
mov dword ptr [ecx], esi
add ecx, 20h
inc edx
cmp ecx, 0040D078h
jl 00007F66CD123F00h
pop edi
xor eax, eax
pop esi
ret
call 00007F66CD124546h
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	0xdaf0	.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
.text	0x1000	0xb1ae	0xb200	False	0.5146374648876404	data	6.0249778256856334	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xd000	0x9098c	0x13400	False	0.9474812297077922	data	7.860179869421139	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.comu	0x9e000	0x96	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x9f000	0xdaf0	0xdc00	False	0.41324573863636366	data	4.47773178292088	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

Name	RVA	Size	Type	Language	Country
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
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

Name	RVA	Size	Type	Language	Country
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	0x258	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, LeaveCriticalSection, GetFileAttributesW, WritePrivateProfileSectionW, TerminateProcess, IsDBCSLeadByte, lstrcmpW, GlobalUnlock, RaiseException, SetCurrentDirectoryA, SetLastError, GetProcAddress, GlobalGetAtomNameA, OpenWaitableTimerA, LocalAlloc, FindFirstVolumeMountPointW, AddAtomA, FindNextFileA, GetModuleHandleA, GetCPInfoExA, SetCalendarInfoA, DeleteFileW, EnumCalendarInfoExA, LocalFree, GetLastError, DeleteFileA, GetCommandLineA, HeapSetInformation, GetStartupInfoW, EnterCriticalSection, 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

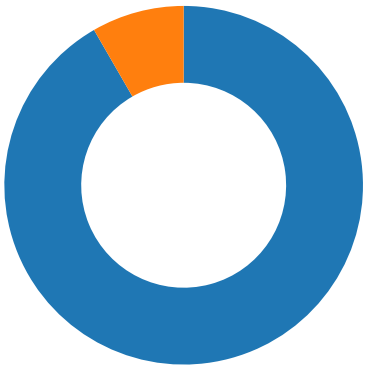
Language of compilation system	Country where language is spoken	Map
Sami Lappish	Finland	
Sami Lappish	Norway	
Sami Lappish	Sweden	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6193.233.175.1 1349705802033204 03/20/23-13:15:36.320401	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49705	80	192.168.2.6	193.233.175.113
192.168.2.662.173.142.81 49704802033203 03/20/23-13:15:16.126464	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49704	80	192.168.2.6	62.173.142.81
192.168.2.662.173.142.81 49704802033204 03/20/23-13:15:16.126464	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49704	80	192.168.2.6	62.173.142.81

Network Port Distribution



Total Packets: 12

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:15:16.062493086 CET	49704	80	192.168.2.6	62.173.142.81
Mar 20, 2023 13:15:16.122262955 CET	80	49704	62.173.142.81	192.168.2.6
Mar 20, 2023 13:15:16.122481108 CET	49704	80	192.168.2.6	62.173.142.81
Mar 20, 2023 13:15:16.126463890 CET	49704	80	192.168.2.6	62.173.142.81
Mar 20, 2023 13:15:16.185555935 CET	80	49704	62.173.142.81	192.168.2.6
Mar 20, 2023 13:15:16.186232090 CET	80	49704	62.173.142.81	192.168.2.6
Mar 20, 2023 13:15:16.186345100 CET	49704	80	192.168.2.6	62.173.142.81
Mar 20, 2023 13:15:16.187962055 CET	49704	80	192.168.2.6	62.173.142.81
Mar 20, 2023 13:15:16.247250080 CET	80	49704	62.173.142.81	192.168.2.6
Mar 20, 2023 13:15:36.216483116 CET	49705	80	192.168.2.6	193.233.175.113
Mar 20, 2023 13:15:36.319710016 CET	80	49705	193.233.175.113	192.168.2.6
Mar 20, 2023 13:15:36.319972038 CET	49705	80	192.168.2.6	193.233.175.113
Mar 20, 2023 13:15:36.320400953 CET	49705	80	192.168.2.6	193.233.175.113
Mar 20, 2023 13:15:36.423428059 CET	80	49705	193.233.175.113	192.168.2.6
Mar 20, 2023 13:15:36.424657106 CET	80	49705	193.233.175.113	192.168.2.6
Mar 20, 2023 13:15:36.424779892 CET	49705	80	192.168.2.6	193.233.175.113
Mar 20, 2023 13:15:36.424930096 CET	49705	80	192.168.2.6	193.233.175.113
Mar 20, 2023 13:15:36.739191055 CET	49705	80	192.168.2.6	193.233.175.113
Mar 20, 2023 13:15:36.842247963 CET	80	49705	193.233.175.113	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:13:55.859003067 CET	49786	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:13:55.886168003 CET	53	49786	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 13:13:55.859003067 CET	192.168.2.6	8.8.8.8	0x5e5a	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 13:13:55.886168003 CET	8.8.8.8	192.168.2.6	0x5e5a	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 62.173.142.81
- 193.233.175.113

Statistics

No statistics

System Behavior

Analysis Process: Server.exe PID: **5744**, Parent PID: **3452**

General

Target ID:	0
Start time:	13:13:41
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:	9565B4A15A8593EA3EC1F3C9D0A2E11A
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: 00000000.00000002.513518394.00000000004E6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.513718671.0000000001FC0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.513908853.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.513908853.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.513908853.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.406328098.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.406328098.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.406328098.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.406192981.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.406192981.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.406192981.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.406310298.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.406310298.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.406310298.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.406101502.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.406101502.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.406101502.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.406169699.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.406169699.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.406169699.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.406228836.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.406228836.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.406228836.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.406261787.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.406261787.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.406261787.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.406142288.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.406142288.0000000002CA8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.406142288.0000000002CA8000.00000004.00000020.00020000.00000000.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