



ID: 830657
Sample Name: server.exe
Cookbook: default.jbs
Time: 15:25:14
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report server.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Compliance 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
System Summary 6
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
Anti Debugging 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Rich Headers 15
Data Directories 15
Sections 15
Resources 15
Imports 17
Possible Origin 17
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 19

Copyright Joe Security LLC 2023

DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 19
Statistics 19
System Behavior 19
Analysis Process: server.exePID: 5776, Parent PID: 3324 19
General 19
File Activities 20
Disassembly 20

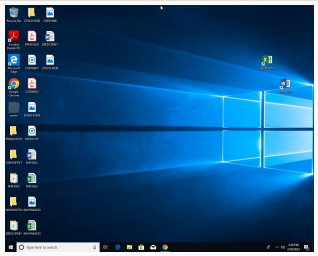
Windows Analysis Report

server.exe

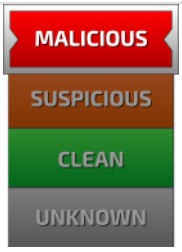
Overview

General Information

Sample Name:	server.exe
Analysis ID:	830657
MD5:	386839452984…
SHA1:	b9c43085f6b63..
SHA256:	f139bc8f71a48…
Tags:	agenziaentrate exe gozi isfb mef mise ursnif
Infos:	



Detection



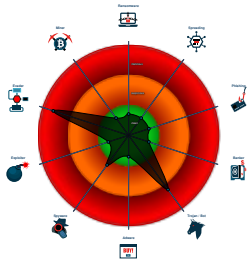
Ursnif

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- server.exe (PID: 5776 cmdline: C:\Users\user\Desktop\server.exe MD5: 386839452984E2EDA4151746D57EA19B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Gozi, Ursnif	2000 Ursnif aka Snifula2006 Gozi v1.0, Gozi CRM, CRM, Papras2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)-> 2010 Gozi Prinimalka -> Vawtrak/NeverquestIn 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed.It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.	No Attribution	http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.htmlhttp://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/gozi-italian-shellcode-dancehttps://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi

Malware Configuration

Threatname: Ursnif

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


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.571809777.0000000000620000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000002.572096214.0000000002F48000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000002.572096214.0000000002F48000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$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
00000000.00000002.572096214.0000000002F48000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x63a:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xa68:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xcf2:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd96:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1cc0:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.455206997.0000000002F48000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

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: 192.168.2.5 - Destination IP: 62.173.142.81

Timestamp:	192.168.2.562.173.142.8149698802033204 03/20/23-15:27:43.098931
SID:	2033204

Copyright Joe Security LLC 2023

Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.5 - Destination IP: 62.173.142.81	−
Timestamp:	192.168.2.562.173.142.8149698802033203 03/20/23-15:27:43.098931
SID:	2033203
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.5 - Destination IP: 193.233.175.113	−
Timestamp:	192.168.2.5193.233.175.11349699802033204 03/20/23-15:28:03.313332
SID:	2033204
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.5 - Destination IP: 193.233.175.113	−
Timestamp:	192.168.2.5193.233.175.11349699802033203 03/20/23-15:28:03.313332
SID:	2033203
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance



Detected unpacking (overwrites its own PE header)

Networking



Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing



Yara detected Ursnif

E-Banking Fraud



Yara detected Ursnif

System Summary



Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation



Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Hooking and other Techniques for Hiding and Protection



Yara detected Ursnif

Malware Analysis System Evasion



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

Anti Debugging



Found API chain indicative of debugger detection

Stealing of Sensitive Information



Yara detected Ursnif

Remote Access Functionality

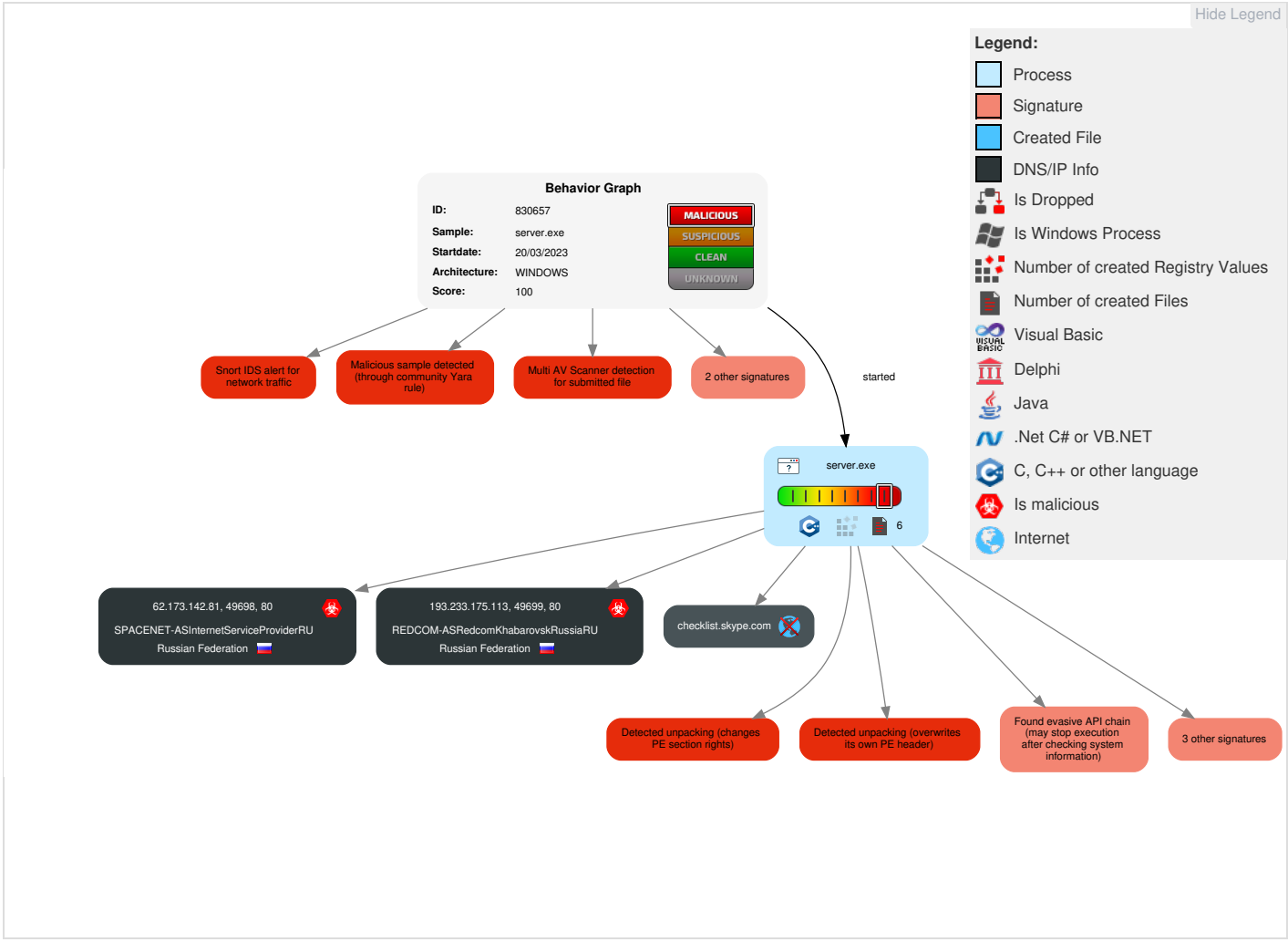


Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Windows Management Instrumentation	Path Interception	Path Interception	1 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

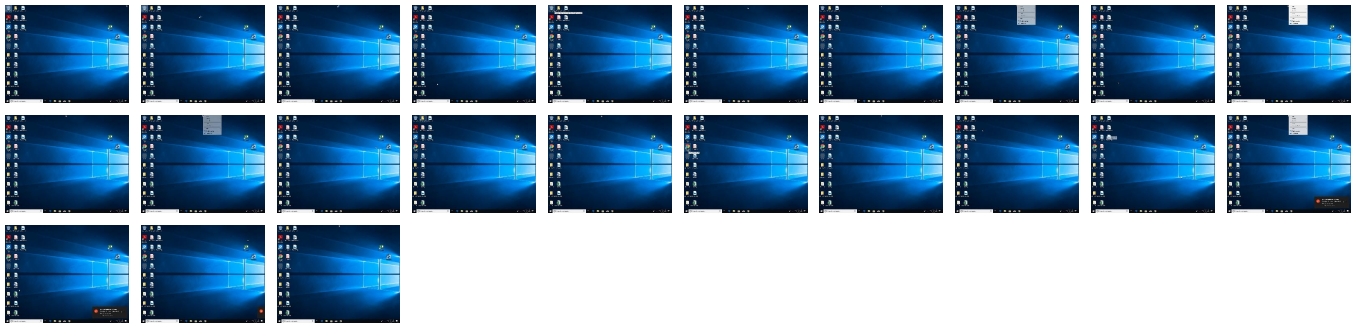
Behavior Graph



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	33%	ReversingLabs		
server.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.server.exe.640000.2.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://193.233.175.113/drew/V9a0o6ef3/Au9_2F9Ppi_2FsgXZknJ/9gyATvTasA37TGnwf_2/FF8_2FeHTfCbmbSNhIELze/nTrHQt_2F5xY5/R3GxHbhE/YI67FVPjLAHvMvQCPm1ZB2r/hUlTXAVF6y/1AwvZRZpD_2BX4_2B/OLj6it5W6CBi/bb63MeG6yuy/QmyD_2FX_2F1Ss/xqhYIyVOpHg2U1VNG_2Fq/xK7Nn_2Fqm4MHDMP/QwAVZmc5HxKcFpM/zNu_2F2WLah1WqJloz/_2Fgr_2B0/Yx87G29pDT1ZwKwi4aHO/N92d2eUOVnKaenJHbAo/y89RoyrX/My.jlk	0%	Avira URL Cloud	safe	
http://62.173.142.81/drew/L41ZdaozWB/9G_2FCBbfzGg7ByXT/_2Bg8QMbKe0e/hoJ4ZQmshRx/yrzS4Fo3MBljQG/zLPIZfVEynjc1_2BzcNzJ/VICSBaC_2BsWiOk3/S_2FVtn98ADwViF/w4EuoTZ6r2ouB5CbJQ/OJAYX7gGB/SPaOx4IeK2WgwzyMW0mh/a6bMYaMIQJb9DwJ1_2B/abyaGtCr0edo_2BHNpcXcS/i41T8cYfwvY4g/ixrgvBpj/x9Y_2FoxbDLce5swL7_2FuZ/twfMwTZOCD/kYv7KY9tblJovwRgo/dob_2F_2FGBd/pRbVJOI3b/HRL7.jlk	0%	Avira URL Cloud	safe	
http://193.23	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

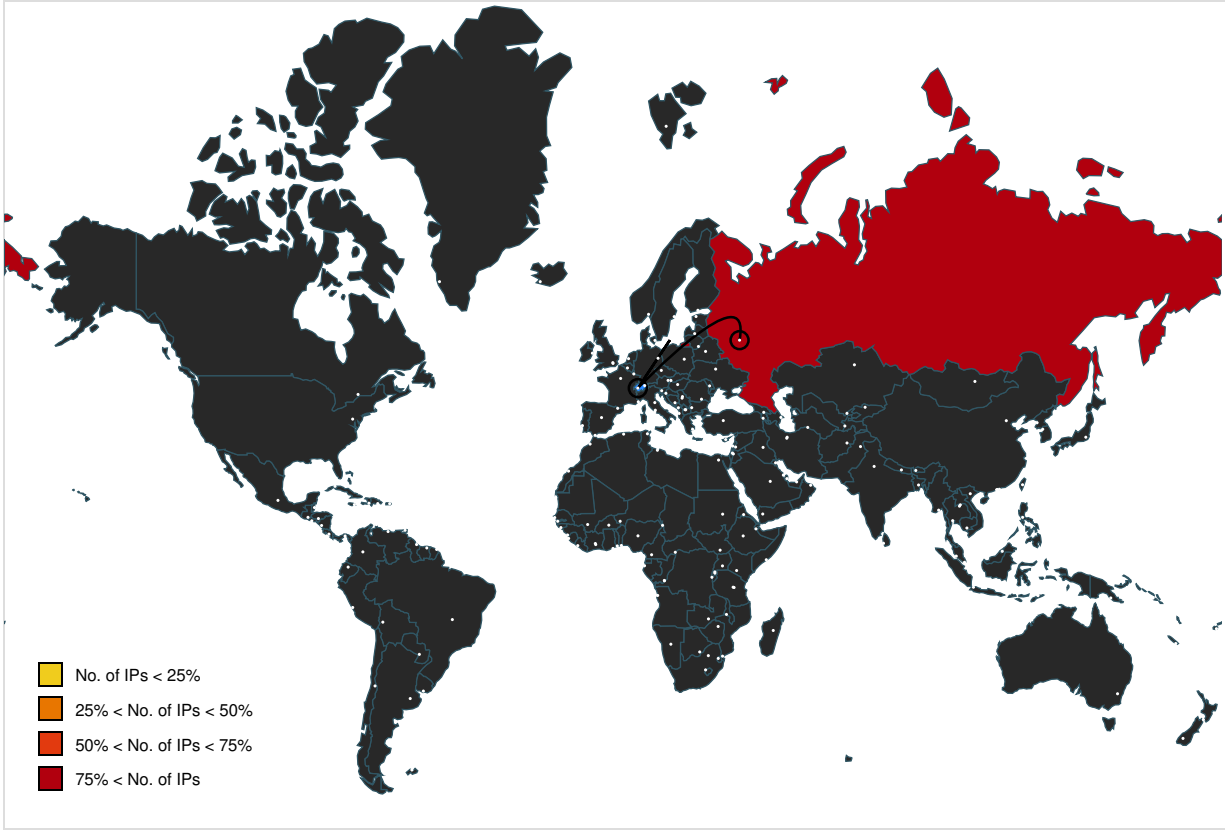
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://193.233.175.113/drew/V9a0o6ef3/Au9_2F9Ppi_2FsgXZknJ/9gyATvTasA37TGnwf_2/FF8_2FeHTfCbmbSNhIELze/nTrHQt_2F5xY5/R3GxHbhE/YI67FVPjLAHvMvQCPm1ZB2r/hUlTXAVF6y/1AwvZRZpD_2BX4_2B/OLj6it5W6CBi/bb63MeG6yuy/QmyD_2FX_2F1Ss/xqhYIyVOpHg2U1VNG_2Fq/xK7Nn_2Fqm4MHDMP/QwAVZmc5HxKcFpM/zNu_2F2WLah1WqJloz/_2Fgr_2B0/Yx87G29pDT1ZwKwi4aHO/N92d2eUOVnKaenJHbAo/y89RoyrX/My.jlk	true	• Avira URL Cloud: safe	unknown
http://62.173.142.81/drew/L41ZdaozWB/9G_2FCBbfzGg7ByXT/_2Bg8QMbKe0e/hoJ4ZQmshRx/yrzS4Fo3MBljQG/zLPIZfVEynjc1_2BzcNzJ/VICSBaC_2BsWiOk3/S_2FVtn98ADwViF/w4EuoTZ6r2ouB5CbJQ/OJAYX7gGB/SPaOx4IeK2WgwzyMW0mh/a6bMYaMIQJb9DwJ1_2B/abyaGtCr0edo_2BHNpcXcS/i41T8cYfwvY4g/ixrgvBpj/x9Y_2FoxbDLce5swL7_2FuZ/twfMwTZOCD/kYv7KY9tblJovwRgo/dob_2F_2FGBd/pRbVJOI3b/HRL7.jlk	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://193.23	server.exe, 00000000.00000002.572075785.00000000029BC000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.173.142.81	unknown	Russian Federation		34300	SPACENET-ASInternetServiceProviderRU	true
193.233.175.113	unknown	Russian Federation		8749	REDCOM-ASRedcomKhabarovskRussiaRU	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830657
Start date and time:	2023-03-20 15:25:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 5s
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@1/2
EGA Information:	• Successful, ratio: 100%

Copyright Joe Security LLC 2023

HDC Information:	• Successful, ratio: 100% (good quality ratio 100%) • Quality average: 89% • Quality standard deviation: 15.4%
HCA Information:	• Successful, ratio: 92% • 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.
- VT rate limit hit for: server.exe

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):	6.788497766819588

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:	182784
MD5:	386839452984e2eda4151746d57ea19b
SHA1:	b9c43085f6b63db8a02b4764c4d75699efa9d074
SHA256:	f139bc8f71a483ba058e2577ef5952b85a74cebd302632a121e4bbc0d96bb953
SHA512:	9a2dd73db8c62f891084d4c47d3edceb2f7eae0113374e9c89d3670dbcb21c98f032b603109a7cad859ad7f3f0c00367e295a8436e3d9749b9ddfe2395151b0d
SSDEEP:	3072:tQPCdvNZmiJN2CE91O6lbP+pnW6ya2wPAnBb4:SavnKO6lz6Tyatw
TLSH:	02048EC353A0BC51F4158A368E2EC2F8671EFC91CE5DAB66E2096F2F48BD162C572741
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....1.a.....

File Icon



Icon Hash:	9aa25a4285aaca82

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:	0x619F31E3 [Thu Nov 25 06:49:07 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	b6299cf22bb1b2b906c76a98a991dd84

Entrypoint Preview

Instruction
call 00007F6404B94BB0h
jmp 00007F6404B921DEh
mov eax, 0040D008h
ret
mov eax, dword ptr [0049D6C0h]
push esi
push 00000014h
pop esi
test eax, eax
jne 00007F6404B92359h
mov eax, 00000200h
jmp 00007F6404B92358h
cmp eax, esi
jnl 00007F6404B92359h
mov eax, esi
mov dword ptr [0049D6C0h], eax
push 00000004h

Instruction
push eax
call 00007F6404B94C5Eh
pop ecx
pop ecx
mov dword ptr [0049C6A0h], eax
test eax, eax
jne 00007F6404B92370h
push 00000004h
push esi
mov dword ptr [0049D6C0h], esi
call 00007F6404B94C45h
pop ecx
pop ecx
mov dword ptr [0049C6A0h], eax
test eax, eax
jne 00007F6404B92357h
push 0000001Ah
pop eax
pop esi
ret
xor edx, edx
mov ecx, 0040D008h
jmp 00007F6404B92357h
mov eax, dword ptr [0049C6A0h]
mov dword ptr [edx+eax], ecx
add ecx, 20h
add edx, 04h
cmp ecx, 0040D288h
jl 00007F6404B9233Ch
push FFFFFFFEh
pop esi
xor edx, edx
mov ecx, 0040D018h
push edi
mov eax, edx
sar eax, 05h
mov eax, dword ptr [0049C5A0h+eax*4]
mov edi, edx
and edi, 1Fh
shl edi, 06h
mov eax, dword ptr [edi+eax]
cmp eax, FFFFFFFFh
je 00007F6404B9235Ah
cmp eax, esi
je 00007F6404B92356h
test eax, eax
jne 00007F6404B92354h
mov dword ptr [ecx], esi
add ecx, 20h
inc edx
cmp ecx, 0040D078h
jl 00007F6404B92320h
pop edi
xor eax, eax
pop esi
ret
call 00007F6404B92966h
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	0xdeb0	.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	0xb1b0	0xb200	False	0.5147252457865169	data	6.025446784943229	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xd000	0x906cc	0x13200	False	0.9445338031045751	data	7.848000030151755	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bujot	0x9e000	0x96	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x9f000	0xdeb0	0xe000	False	0.412109375	data	4.481548452883521	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0xab608	0x2	data		
TONIZITOHOWAPEVUMOBEM	0xaaf10	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Finland
TONIZITOHOWAPEVUMOBEM	0xaaf10	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Norway
TONIZITOHOWAPEVUMOBEM	0xaaf10	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Sweden
RT_CURSOR	0xab610	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xab740	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0xab830	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x9f6f0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0x9f6f0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0x9f6f0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0x9ff98	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland

Copyright Joe Security LLC 2023

Name	RVA	Size	Type	Language	Country
RT_ICON	0x9ff98	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0x9ff98	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa1068	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa1068	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa1068	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa1910	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa1910	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa1910	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa3eb8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa3eb8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa3eb8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa4f90	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa4f90	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa4f90	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa5e38	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa5e38	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa5e38	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa6500	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa6500	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa6500	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa6a68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa6a68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa6a68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa9010	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa9010	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa9010	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xaa0b8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xaa0b8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xaa0b8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xaaa40	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xaaa40	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xaaa40	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Sweden
RT_STRING	0xacb58	0x29c	data	Sami Lappish	Finland
RT_STRING	0xacb58	0x29c	data	Sami Lappish	Norway
RT_STRING	0xacb58	0x29c	data	Sami Lappish	Sweden
RT_STRING	0xacdf8	0xb6	data	Sami Lappish	Finland
RT_STRING	0xacdf8	0xb6	data	Sami Lappish	Norway
RT_STRING	0xacdf8	0xb6	data	Sami Lappish	Sweden

Copyright Joe Security LLC 2023

Name	RVA	Size	Type	Language	Country
RT_ACCELERATOR	0xab550	0x78	data	Sami Lappish	Finland
RT_ACCELERATOR	0xab550	0x78	data	Sami Lappish	Norway
RT_ACCELERATOR	0xab550	0x78	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xab4a8	0xa8	data	Sami Lappish	Finland
RT_ACCELERATOR	0xab4a8	0xa8	data	Sami Lappish	Norway
RT_ACCELERATOR	0xab4a8	0xa8	data	Sami Lappish	Sweden
RT_GROUP_CURSOR	0xac8d8	0x30	data		
RT_GROUP_ICON	0xa4f60	0x30	data	Sami Lappish	Finland
RT_GROUP_ICON	0xa4f60	0x30	data	Sami Lappish	Norway
RT_GROUP_ICON	0xa4f60	0x30	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xa1040	0x22	data	Sami Lappish	Finland
RT_GROUP_ICON	0xa1040	0x22	data	Sami Lappish	Norway
RT_GROUP_ICON	0xa1040	0x22	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xaaea8	0x68	data	Sami Lappish	Finland
RT_GROUP_ICON	0xaaea8	0x68	data	Sami Lappish	Norway
RT_GROUP_ICON	0xaaea8	0x68	data	Sami Lappish	Sweden
RT_VERSION	0xac908	0x24c	data		
None	0xab5c8	0xa	data	Sami Lappish	Finland
None	0xab5c8	0xa	data	Sami Lappish	Norway
None	0xab5c8	0xa	data	Sami Lappish	Sweden
None	0xab5d8	0xa	data	Sami Lappish	Finland
None	0xab5d8	0xa	data	Sami Lappish	Norway
None	0xab5d8	0xa	data	Sami Lappish	Sweden
None	0xab5e8	0xa	data	Sami Lappish	Finland
None	0xab5e8	0xa	data	Sami Lappish	Norway
None	0xab5e8	0xa	data	Sami Lappish	Sweden
None	0xab5f8	0xa	data	Sami Lappish	Finland
None	0xab5f8	0xa	data	Sami Lappish	Norway
None	0xab5f8	0xa	data	Sami Lappish	Sweden

Imports

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

Possible Origin

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

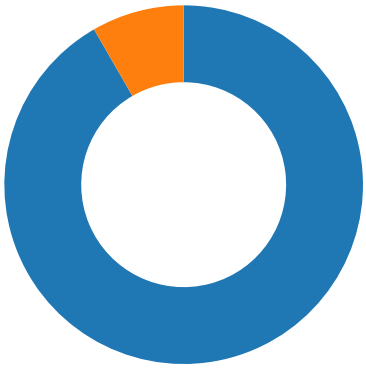
Language of compilation system	Country where language is spoken	Map
Sami Lappish	Sweden	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.562.173.142.81 49698802033204 03/20/23-15:27:43.098931	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49698	80	192.168.2.5	62.173.142.81
192.168.2.562.173.142.81 49698802033203 03/20/23-15:27:43.098931	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49698	80	192.168.2.5	62.173.142.81
192.168.2.5193.233.175.1 1349699802033204 03/20/23-15:28:03.313332	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49699	80	192.168.2.5	193.233.175.113
192.168.2.5193.233.175.1 1349699802033203 03/20/23-15:28:03.313332	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49699	80	192.168.2.5	193.233.175.113

Network Port Distribution



Total Packets: 12

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 15:27:43.033325911 CET	49698	80	192.168.2.5	62.173.142.81
Mar 20, 2023 15:27:43.097949028 CET	80	49698	62.173.142.81	192.168.2.5
Mar 20, 2023 15:27:43.098150015 CET	49698	80	192.168.2.5	62.173.142.81
Mar 20, 2023 15:27:43.098931074 CET	49698	80	192.168.2.5	62.173.142.81
Mar 20, 2023 15:27:43.162194014 CET	80	49698	62.173.142.81	192.168.2.5
Mar 20, 2023 15:27:43.162780046 CET	80	49698	62.173.142.81	192.168.2.5
Mar 20, 2023 15:27:43.162868023 CET	49698	80	192.168.2.5	62.173.142.81
Mar 20, 2023 15:27:43.165563107 CET	49698	80	192.168.2.5	62.173.142.81
Mar 20, 2023 15:27:43.230212927 CET	80	49698	62.173.142.81	192.168.2.5
Mar 20, 2023 15:28:03.200493097 CET	49699	80	192.168.2.5	193.233.175.113
Mar 20, 2023 15:28:03.304471970 CET	80	49699	193.233.175.113	192.168.2.5
Mar 20, 2023 15:28:03.306303978 CET	49699	80	192.168.2.5	193.233.175.113

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 15:28:03.313332081 CET	49699	80	192.168.2.5	193.233.175.113
Mar 20, 2023 15:28:03.416959047 CET	80	49699	193.233.175.113	192.168.2.5
Mar 20, 2023 15:28:03.417373896 CET	80	49699	193.233.175.113	192.168.2.5
Mar 20, 2023 15:28:03.417480946 CET	49699	80	192.168.2.5	193.233.175.113
Mar 20, 2023 15:28:03.417574883 CET	49699	80	192.168.2.5	193.233.175.113
Mar 20, 2023 15:28:03.759030104 CET	49699	80	192.168.2.5	193.233.175.113
Mar 20, 2023 15:28:03.862701893 CET	80	49699	193.233.175.113	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 15:26:22.885719061 CET	50295	53	192.168.2.5	8.8.8.8
Mar 20, 2023 15:26:22.913109064 CET	53	50295	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 20, 2023 15:26:22.885719061 CET	192.168.2.5	8.8.8.8	0x636c	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 15:26:22.913109064 CET	8.8.8.8	192.168.2.5	0x636c	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: **5776**, Parent PID: **3324**

General

Target ID:	0
Start time:	15:26:12
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:	182784 bytes
MD5 hash:	386839452984E2EDA4151746D57EA19B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.571809777.0000000000620000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.572096214.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.572096214.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.572096214.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.455206997.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.455206997.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.455206997.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.455025365.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.455025365.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.455025365.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.455061922.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.455061922.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.455061922.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.455168665.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.455168665.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.455168665.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.571863251.0000000000676000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.455217317.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.455217317.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.455217317.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.455118106.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.455118106.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.455118106.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.455147068.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.455147068.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.455147068.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.455087748.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.455087748.0000000002F48000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.455087748.0000000002F48000.00000004.00000020.00020000.00000000.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