ID: 827096
Sample Name: server.exe
Cookbook: default.jbs
Time: 15:17:20
Date: 15/03/2023
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
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
System Summary 6
Data Obfuscation 6
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
Anti Debugging 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
General 11
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Rich Headers 14
Data Directories 14
Sections 14
Resources 14
Imports 16
Possible Origin 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 17

HTTP Request Dependency Graph 17
Statistics 17
System Behavior 17
Analysis Process: server.exePID: 5284, Parent PID: 3528 17
General 17
File Activities 18
Disassembly 18

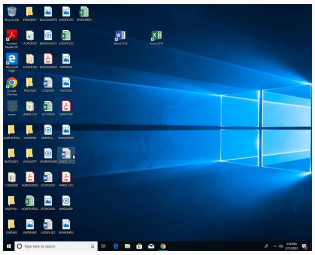
Windows Analysis Report

server.exe

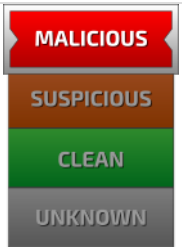
Overview

General Information

Sample Name:	server.exe
Analysis ID:	827096
MD5:	d966642aac4f2..
SHA1:	c841e25cf191d..
SHA256:	38befee4c4513..
Tags:	agenziaentrate exe gozi isfb ITA mef mise ursnif
Infos:	



Detection



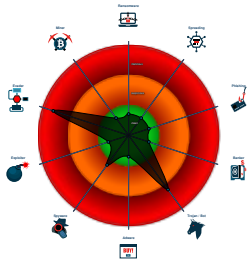
Ursnif

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…
- Uses 32bit PE files
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- server.exe (PID: 5284 cmdline: C:\Users\user\Desktop\server.exe MD5: D966642AAC4F23E0EC3CB978B949FD9D)
- **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":
"ScCitKVnthsrIejolA7zuBWvwII2di/DH3GlyTtkQAl5+NYn11P8hoApgIAx8QgiEaRicK3ETZq3j2ua44XjJevEH0XzzTqZAT3wkYswDxrBkgZMCwo6YXkhXitvoh3eARDtRDEkQsoLHZ9GnSskgPPZhcXZcW5DEVGUxmtbXgDaTXEE
ASp94TxsSTq8LcHFcoUD/3qCUIKISKD7sIV0hgpJQ8kx5Fr/zREoX54YDyuxKi/xJ3SBIavWF9UPU+YwvxpBDYMFrMsKJrjGUlpoQZehisJjttb1cTtggelEGnFr5O2GXefQUuwrSizDeVnMRSAHdds+AiqlPxEl1nFzSfnHhHtw7Ql8J
tPTws7Z1Ho=",
  "c2_domain": [
    "checklist.skype.com",
    "5.44.43.17",
    "31.41.44.108",
    "62.173.138.213",
    "109.248.11.174"
  ],
  "botnet": "7714",
  "server": "50",
  "serpent_key": "lk8hY4nisKQzZKXE",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.583476468.0000000002BC8000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x6af3:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000003.475989418.00000000053D8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.475989418.00000000053D8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$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
00000000.00000003.475989418.00000000053D8000.00000004.00000020.00020000.00000000.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:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1ca0:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.476024280.00000000053D8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 27 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

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

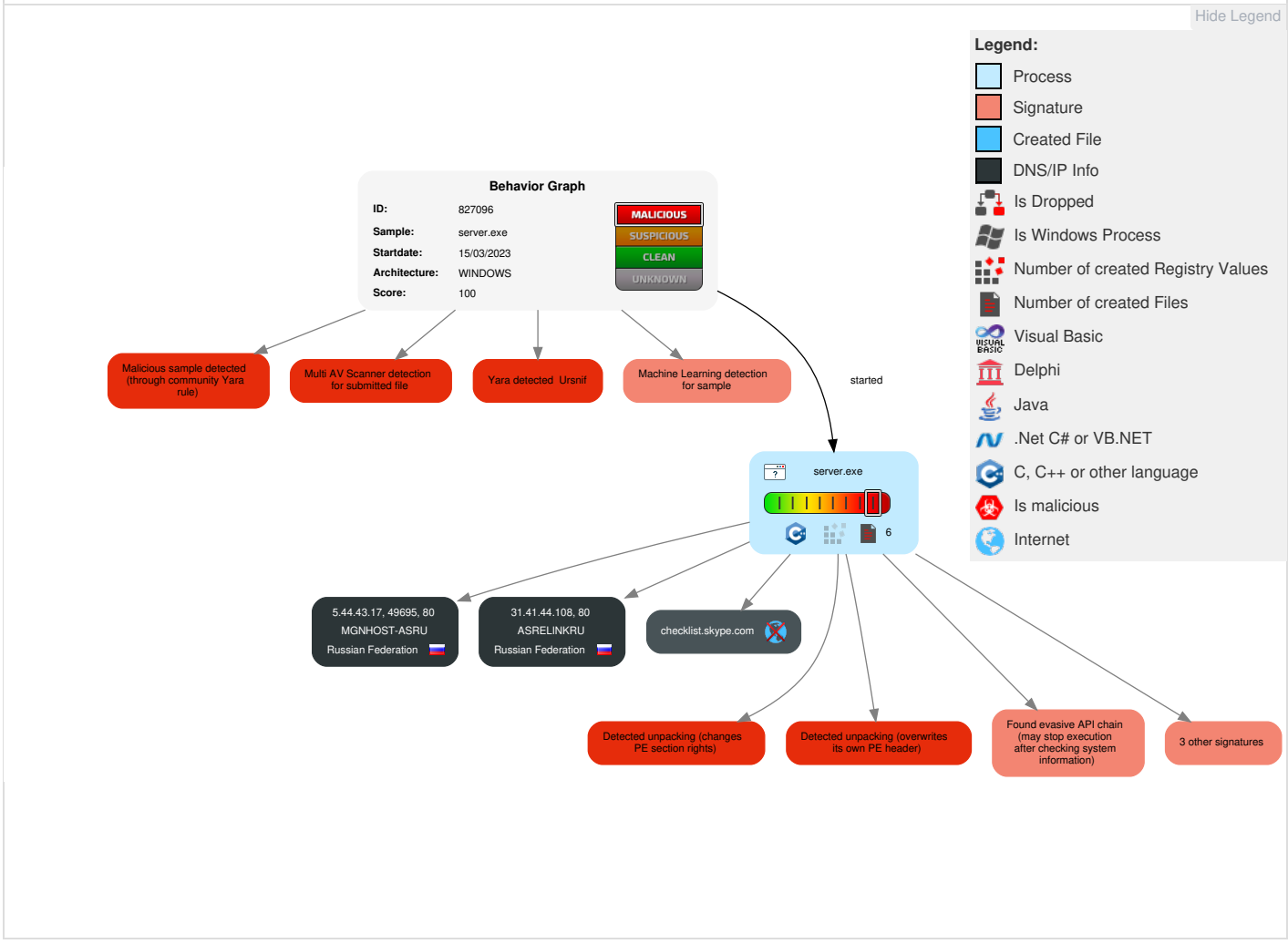
Remote Access Functionality

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 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

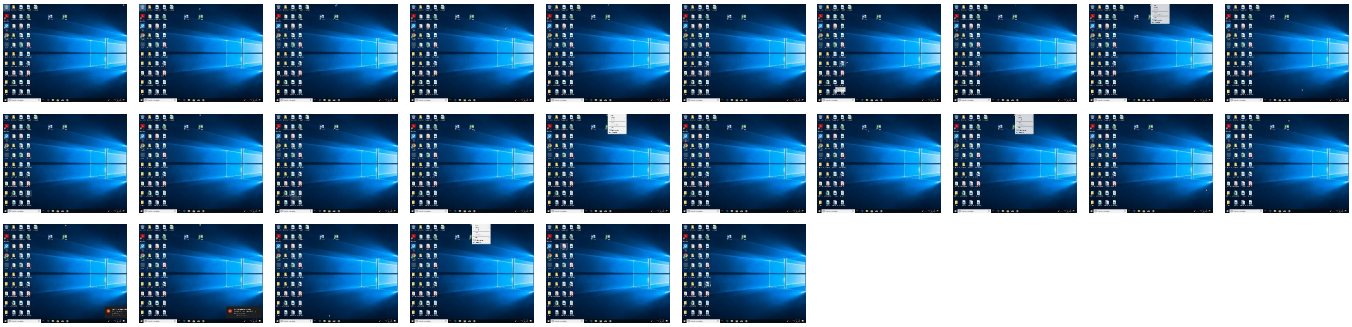
Behavior Graph



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	38%	ReversingLabs	Win32.Ransomware.Stop	
server.exe	54%	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.2b90000.2.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://31.41.	0%	Virustotal		Browse
http://5.44.43.17/drew/f9GHjdJnehl_2BX/Ne5g2ordmIOToC91gh/mNbzuN3c2/5AW_2FtlsPkVoHj0AzU6/Pm6UGSYAVX5awiiNdCX/eNOyKJzs_2F6vuQoDvWCQ0/1kQi8Yq7709M2/upQopQi2/s9QJW0HP19fXNX5NpkaC7rS/XtTUHeQq7L/Mwx2fdHiqqVJlhw5T/ErHqsGRIPLQF/P1EQ7mB71HQ/eppTj5uvam1edz/PvmLkUCCoHuafjeSLYKxe/uQzSahqYp69cTJ2o/M6RFmPe3MSlVrTk/KwEVVAo6CnR9Fpgg/f20Iv.jlk	0%	Avira URL Cloud	safe	
http://31.41.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

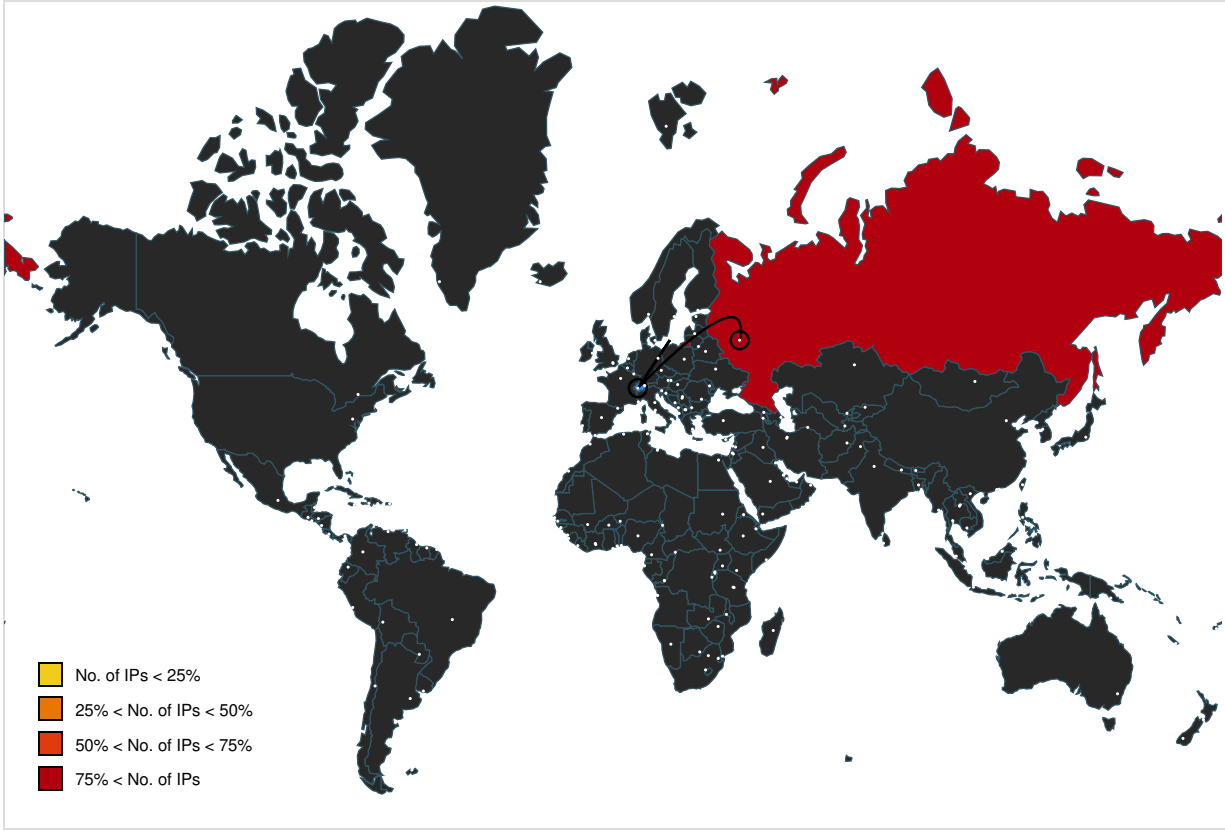
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://5.44.43.17/drew/f9GHjdJnehl_2BX/Ne5g2ordmIOToC91gh/mNbzuN3c2/5AW_2FtlsPkVoHj0AzU6/Pm6UGSYAVX5awiiNdCX/eNOyKJzs_2F6vuQoDvWCQ0/1kQi8Yq7709M2/upQopQi2/s9QJW0HP19fXNX5NpkaC7rS/XtTUHeQq7L/Mwx2fdHiqqVJlhw5T/ErHqsGRIPLQF/P1EQ7mB71HQ/eppTj5uvam1edz/PvmLkUCCoHuafjeSLYKxe/uQzSahqYp69cTJ2o/M6RFmPe3MSlVrTk/KwEVVAo6CnR9Fpgg/f20Iv.jlk	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://31.41.	server.exe, 00000000.00000002.583568849.00000000048AC000.00000004.00000010.00020000.00000000.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
5.44.43.17	unknown	Russian Federation		202423	MGNHOST-ASRU	false
31.41.44.108	unknown	Russian Federation		56577	ASRELINKRU	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	827096
Start date and time:	2023-03-15 15:17:20 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
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:	7
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: 31.1% (good quality ratio 31.1%) • Quality average: 89% • Quality standard deviation: 15.4%

HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe
- 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):	6.1366949871889025
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:	307200
MD5:	d966642aac4f23e0ec3cb978b949fd9d
SHA1:	c841e25cf191d5a327d6917731333d61f7b4ad0d
SHA256:	38befee4c4513de47e667544d9f705f56c195393b116fcd154755c1f7815ae55
SHA512:	03f49e1eeb72b3786fe207cc688439f66877cd6afb2ecc1b60e32aaa25fe6992c663ebb970a7e53cf9bb13ccff1b2471ff1be2280ff292e237b30ee487f23be1
SSDEEP:	3072:+QbWTLHiq9HunZr2ADhW8c/S9OC1hE/uJuP8QrW7SNlfo:pbiL31uAKR9p02p9ae
TLSH:	6F641A0392E1BC85E92A8B739E2FD6F8775EF6508E49776922289F1F44B0076C273711
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~:..:[..:[..:[..$.>..[..$./..[..$.9.Y[.....3[..:[..K[..$.0.;[..$...;[..$.+.;[..Rich:[.....PE..L.....7b...

File Icon

Icon Hash:	a4a4a094a4b4a4e0

Static PE Info

General

Entrypoint:	0x404e18
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x623706BE [Sun Mar 20 10:49:34 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	02bcb533fc6eab16fabdf3b7ff49a9d9

Entrypoint Preview

Instruction
call 00007F81DCB96EF4h
jmp 00007F81DCB94F3Eh
mov edi, edi
push ecx
mov dword ptr [ecx], 0040125Ch
call 00007F81DCB96F77h
pop ecx
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, ecx
call 00007F81DCB950A8h
test byte ptr [ebp+08h], 00000001h
je 00007F81DCB950C9h
push esi
call 00007F81DCB95373h
pop ecx
mov eax, esi
pop esi

Instruction
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
mov ecx, dword ptr [ebp+08h]
push ebx
xor ebx, ebx
push esi
push edi
cmp ecx, ebx
je 00007F81DCB950C9h
mov edi, dword ptr [ebp+0Ch]
cmp edi, ebx
jnbe 00007F81DCB950DDh
call 00007F81DCB971DCh
push 00000016h
pop esi
mov dword ptr [eax], esi
push ebx
push ebx
push ebx
push ebx
push ebx
call 00007F81DCB97165h
add esp, 14h
mov eax, esi
jmp 00007F81DCB950F2h
mov esi, dword ptr [ebp+10h]
cmp esi, ebx
jne 00007F81DCB950C6h
mov byte ptr [ecx], bl
jmp 00007F81DCB9509Ch
mov edx, ecx
mov al, byte ptr [esi]
mov byte ptr [edx], al
inc edx
inc esi
cmp al, bl
je 00007F81DCB950C5h
dec edi
jne 00007F81DCB950B5h
cmp edi, ebx
jne 00007F81DCB950D2h
mov byte ptr [ecx], bl
call 00007F81DCB971A1h
push 00000022h
pop ecx
mov dword ptr [eax], ecx
mov esi, ecx
jmp 00007F81DCB95083h
xor eax, eax
pop edi
pop esi
pop ebx
pop ebp
ret
push 0000000Ch
push 0040EEA0h

Instruction
call 00007F81DCB96C56h
and dword ptr [ebp-1Ch], 00000000h
mov esi, dword ptr [ebp+08h]
cmp esi, dword ptr [02AE85B0h]
jnbe 00007F81DCB950E4h
push 00000004h
call 00007F81DCB972FEh
pop ecx
and dword ptr [ebp+00h], 00000000h

Rich Headers

Programming Language:	• [C++] VS2008 build 21022 • [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf14c	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26e9000	0x1d478	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2707000	0xa3c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11c0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2d98	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x17c	.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	0xe9f2	0xea00	False	0.587623530982906	data	6.759089266347376	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x10000	0x26d8704	0x17200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x26e9000	0x1d478	0x1d600	False	0.39876994680851063	data	4.4647897989049445	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2707000	0x78d8	0x7a00	False	0.0756595799180328	data	0.9342098464691151	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x2702ba0	0x330	Device independent bitmap graphic, 48 x 96 x 1, image size 0		
RT_CURSOR	0x2702ed0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x2703028	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_CURSOR	0x2703ed0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x2704778	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_CURSOR	0x2704d10	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x2704e40	0xb0	Device independent bitmap graphic, 16 x 32 x 1, image size 0		
RT_ICON	0x26e9ac0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Serbian	Italy
RT_ICON	0x26ea968	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Serbian	Italy
RT_ICON	0x26eb210	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Serbian	Italy
RT_ICON	0x26eb8d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Serbian	Italy
RT_ICON	0x26ebe40	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Serbian	Italy
RT_ICON	0x26ee3e8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Serbian	Italy
RT_ICON	0x26ef490	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Serbian	Italy
RT_ICON	0x26ef960	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Serbian	Italy
RT_ICON	0x26f0808	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Serbian	Italy
RT_ICON	0x26f10b0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Serbian	Italy
RT_ICON	0x26f1778	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Serbian	Italy
RT_ICON	0x26f1ce0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Serbian	Italy
RT_ICON	0x26f4288	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Serbian	Italy
RT_ICON	0x26f5330	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Serbian	Italy
RT_ICON	0x26f5cb8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Serbian	Italy
RT_ICON	0x26f6198	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Serbian	Italy
RT_ICON	0x26f7040	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Serbian	Italy
RT_ICON	0x26f78e8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Serbian	Italy
RT_ICON	0x26f7e50	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Serbian	Italy
RT_ICON	0x26fa3f8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Serbian	Italy
RT_ICON	0x26fb4a0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Serbian	Italy
RT_ICON	0x26fbe28	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Serbian	Italy
RT_ICON	0x26fc2f8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Serbian	Italy
RT_ICON	0x26fd1a0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Serbian	Italy
RT_ICON	0x26fda48	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Serbian	Italy
RT_ICON	0x26fe110	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Serbian	Italy
RT_ICON	0x26fe678	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Serbian	Italy
RT_ICON	0x2700c20	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Serbian	Italy
RT_ICON	0x2701cc8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Serbian	Italy
RT_ICON	0x2702650	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Serbian	Italy
RT_STRING	0x2705110	0x2be	data		
RT_STRING	0x27053d0	0x492	data		
RT_STRING	0x2705868	0x5c6	data		
RT_STRING	0x2705e30	0x118	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x2705f48	0x52a	data		
RT_ACCELERATOR	0x2702b30	0x48	data	Serbian	Italy
RT_ACCELERATOR	0x2702b78	0x18	data	Serbian	Italy
RT_GROUP_CURSOR	0x2703000	0x22	data		
RT_GROUP_CURSOR	0x2704ce0	0x30	data		
RT_GROUP_CURSOR	0x2704ef0	0x22	data		
RT_GROUP_ICON	0x26fc290	0x68	data	Serbian	Italy
RT_GROUP_ICON	0x26ef8f8	0x68	data	Serbian	Italy
RT_GROUP_ICON	0x26f6120	0x76	data	Serbian	Italy
RT_GROUP_ICON	0x2702ab8	0x76	data	Serbian	Italy
RT_VERSION	0x2704f18	0x1f8	data		
None	0x2702b90	0xa	data		

Imports

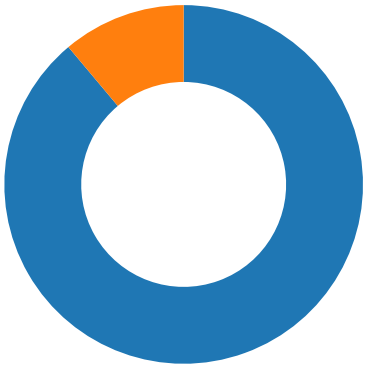
DLL	Import
KERNEL32.dll	CreateHardLinkA, CallNamedPipeW, GetCommConfig, GetConsoleAliasesA, GetWindowsDirectoryA, FindResourceExA, GlobalAlloc, WideCharToMultiByte, LoadLibraryW, GetStringTypeExW, GetExitCodeProcess, lstrcpynW, GetFileAttributesW, LocalReAlloc, WriteConsoleW, GetBinaryTypeA, SetLastError, GetProcAddress, VirtualAlloc, FindCloseChangeNotification, EnumSystemCodePagesW, GetFileType, CreateEventW, EnumDateFormatsA, FreeEnvironmentStringsW, GetPrivateProfileSectionA, GetStringTypeW, FindAtomW, DeleteTimerQueueTimer, GlobalAddAtomW, OpenFileMappingA, LCMapStringW, HeapSize, OpenJobObjectA, GetStartupInfoW, HeapAlloc, GetLastError, HeapFree, SetUnhandledExceptionFilter, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, GetModuleFileNameW, GetEnvironmentStringsW, GetCommandLineW, SetHandleCount, GetStartupInfoA, DeleteCriticalSection, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, IsDebuggerPresent, LeaveCriticalSection, EnterCriticalSection, HeapReAlloc, RaiseException, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LoadLibraryA, InitializeCriticalSectionAndSpinCount, RtlUnwind, GetModuleHandleA, LCMapStringA, MultiByteToWideChar, GetStringTypeA, GetLocaleInfoA
USER32.dll	CreateMDIWindowA, LoadMenuW, GetMenuInfo, ValidateRect, NotifyWinEvent
GDI32.dll	GetGlyphIndicesA
ADVAPI32.dll	MapGenericMask

Possible Origin

Language of compilation system	Country where language is spoken	Map
Serbian	Italy	

Network Behavior

Network Port Distribution



Total Packets: 9

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 15, 2023 15:19:56.314440012 CET	49695	80	192.168.2.4	5.44.43.17
Mar 15, 2023 15:19:56.368020058 CET	80	49695	5.44.43.17	192.168.2.4
Mar 15, 2023 15:19:56.368206024 CET	49695	80	192.168.2.4	5.44.43.17
Mar 15, 2023 15:19:56.371812105 CET	49695	80	192.168.2.4	5.44.43.17
Mar 15, 2023 15:19:56.425127983 CET	80	49695	5.44.43.17	192.168.2.4
Mar 15, 2023 15:19:56.426049948 CET	80	49695	5.44.43.17	192.168.2.4
Mar 15, 2023 15:19:56.426125050 CET	49695	80	192.168.2.4	5.44.43.17
Mar 15, 2023 15:19:56.431993961 CET	49695	80	192.168.2.4	5.44.43.17
Mar 15, 2023 15:19:56.485348940 CET	80	49695	5.44.43.17	192.168.2.4
Mar 15, 2023 15:20:16.470371962 CET	49696	80	192.168.2.4	31.41.44.108
Mar 15, 2023 15:20:19.485114098 CET	49696	80	192.168.2.4	31.41.44.108
Mar 15, 2023 15:20:25.485605955 CET	49696	80	192.168.2.4	31.41.44.108

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 15, 2023 15:18:35.357211113 CET	56572	53	192.168.2.4	8.8.8.8
Mar 15, 2023 15:18:35.421377897 CET	53	56572	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 15, 2023 15:18:35.357211113 CET	192.168.2.4	8.8.8.8	0xd897	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 15, 2023 15:18:35.421377897 CET	8.8.8.8	192.168.2.4	0xd897	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 5.44.43.17

Statistics

No statistics

System Behavior

Analysis Process: server.exe PID: 5284, Parent PID: 3528

General

Target ID:	0
Start time:	15:18:19
Start date:	15/03/2023
Path:	C:\Users\user\Desktop\server.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\server.exe
Imagebase:	0x400000

File size:	307200 bytes
MD5 hash:	D966642AAC4F23E0EC3CB978B949FD9D
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: 00000000.00000002.583476468.0000000002BC8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.475989418.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.475989418.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.475989418.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.476024280.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.476024280.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.476024280.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.583410060.0000000002B20000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.583665066.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.583665066.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.583665066.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.475926489.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.475926489.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.475926489.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.476053706.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.476053706.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.476053706.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.475966518.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.475966518.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.475966518.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.476093791.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.476093791.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.476093791.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.475856834.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.475856834.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.475856834.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.475894970.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.475894970.00000000053D8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.475894970.00000000053D8000.00000004.00000020.00020000.00000000.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