ID: 826138
Sample Name: server.exe
Cookbook: default.jbs
Time: 12:25:09
Date: 14/03/2023
Version: 37.0.0 Beryl

Table of Contents

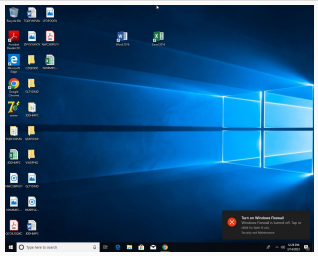
Windows Analysis Report

server.exe

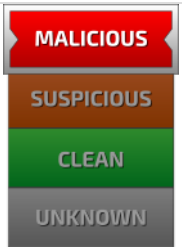
Overview

General Information

Sample Name:	server.exe
Analysis ID:	826138
MD5:	43cfce2e126b1..
SHA1:	9ca60bfc3cb13..
SHA256:	47d288233a39...
Tags:	agenziaentrate exe gozi isfb ITA mef mise ursnif
Infos:	



Detection



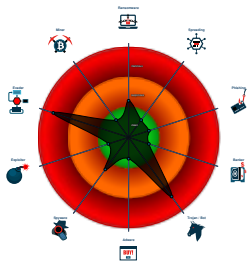
Ursnif, CryptOne

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

Signatures

- Multi AV Scanner detection for subm...
- Detected unpacking (changes PE se...
- Icon mismatch, binary includes an i...
- Malicious sample detected (through...
- Detected unpacking (overwrites its o...
- Yara detected CryptOne packer
- 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...

Classification



Process Tree

- **System is w10x64**
- server.exe (PID: 5596 cmdline: C:\Users\user\Desktop\server.exe MD5: 43CFCE2E126B1BF5230E51EDD205F6BD)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Gozi, Ursnif	2000 Ursnif aka Snifula2006 Gozi v1.0, Gozi CRM, CRM, Papras2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)-> 2010 Gozi Prinimalka -> Vawtrak/NeverquestIn 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed.It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.	No Attribution	http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.htmlhttp://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"2cHitNE2khtX8MPowN3OuEF+nIJiRQvDS0CByWczHAmlx7InAyPYhqz4W4BdwOQhPXM+cNmTKZrjXkeaD1W/JReU+0QfnRaZLQzMkbf/6hntYeJLN9kVYaXwOSubcfndLd/IRF3zHco37HpGyfr/fx+pYcUFQUpDPSBwxpcqOgAGHU0E
LflY4Wg7JTro/JzFnlTf/qZRLIK0F3z73FRQhjYYH8ldszb/+eADX8rn6ird+QrxU0NdIdel89Q7IsIw6+kcDa/Uh8s29ZPGfilEQcNwZsKPhbL1nQo8gRUU9nCXs8mGibasUhj7JSzvSDXMce/idAcO3inRDu0kAkFPSSWXYHucvOV7U
qKvwvqosHo=",
  "c2_domain": [
    "checklist.skype.com",
    "62.173.142.51",
    "94.103.183.153",
    "193.233.175.111",
    "109.248.11.145",
    "31.41.44.106",
    "191.96.251.201"
  ],
  "botnet": "7713",
  "server": "50",
  "serpent_key": "rqDYWFa4uPXuBFMj",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.569302533.0000000002190000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_CryptOne	Yara detected CryptOne packer	Joe Security	
00000000.00000003.446824514.00000000035B8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.446824514.00000000035B8000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.446824514.00000000035B8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x63a:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xa68:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xcf2:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd96:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1ce8:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000002.569534669.00000000035B8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 5 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 62.173.142.51

Timestamp:	192.168.2.462.173.142.5149685802033203 03/14/23-12:27:29.882824
SID:	2033203

Source Port:	49685
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

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

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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 CryptOne packer

Yara detected Ursnif

Remote Access Functionality

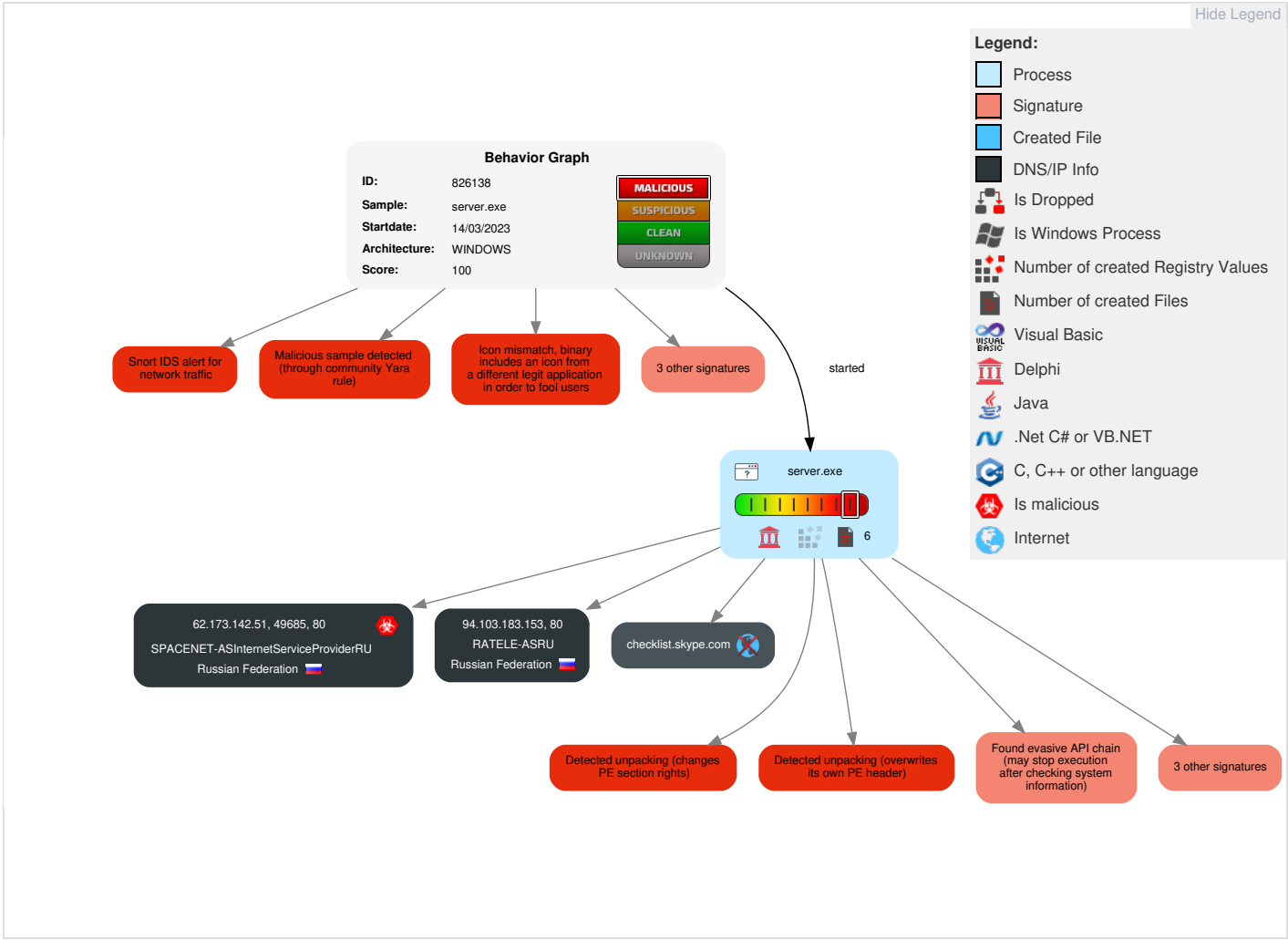
Yara detected CryptOne packer

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 Masquerading	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 Virtualization/Sandbox Evasion	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)	1 Disable or Modify Tools	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)	1 Obfuscated Files or Information	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	2 1 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	13%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.server.exe.2bd0000.3.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
0.2.server.exe.2190174.1.unpack	100%	Avira	TR/Kazy.4159236		Download File
0.2.server.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://62.173.142.51/drew/HAyCvnAuEOt2F7C/qtqWyxm4JAodLmr2fA/5rIXi6c7a/A8VZuoBaw9m9tdhD88nR/7GG7oRWMVub4oY7_2BO/OtqOu0B56I1LS_2FdHx85_/2FJqjErmgnBnc/fR5wyLVd/zR03KdsDmrJhOpNTELG8Ap7/tRbeA0rm1D/Ahqeb_2B_2Fx66NAH/sAJz2fkfv30m/_2B2yXv1C0u/OTAlb_2Bjz3Xu9/n7nMr5QIveWoLOKJgWpZZ/FZTPBpvOXNqs9vrA/ayBpSg1Jbp3hq/vUJdeVU7/u.jlk	0%	Avira URL Cloud	safe	
http://94.103	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

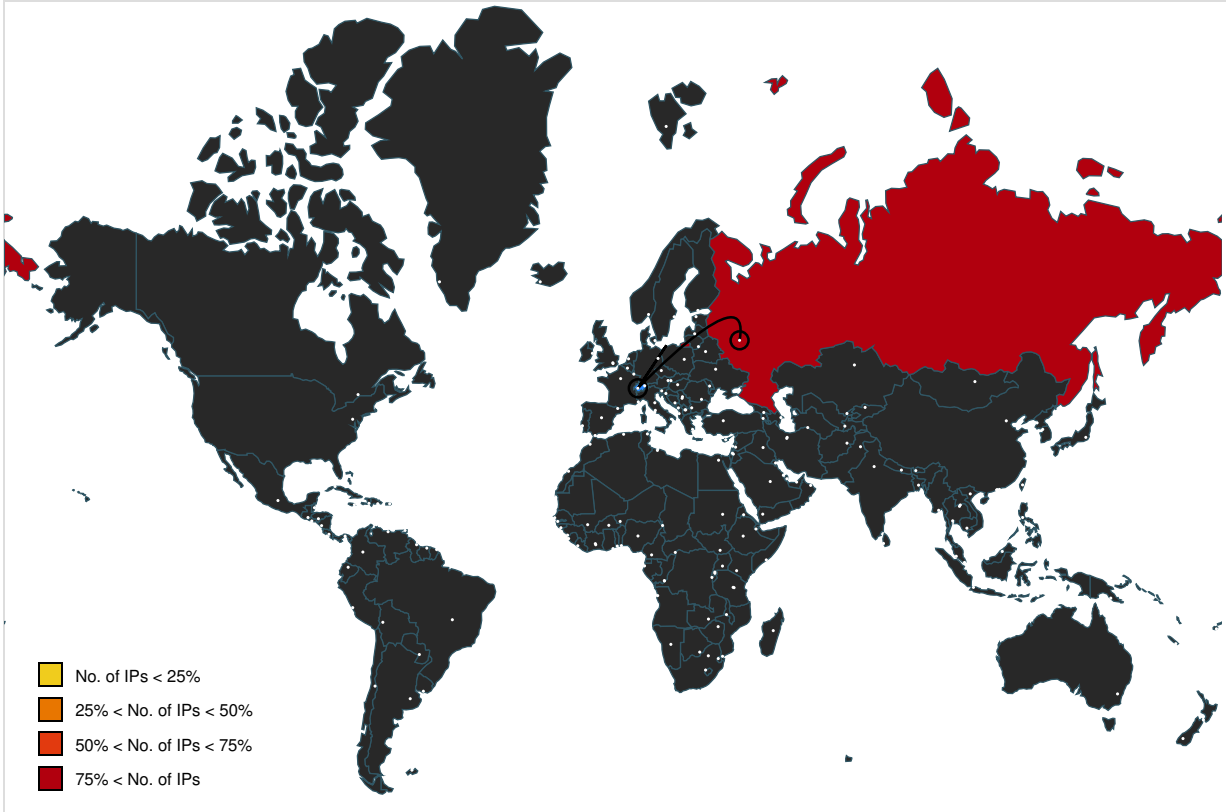
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://62.173.142.51/drew/HAyCvnAuEOt2F7C/qtqWyxm4JAodLmr2fA/5rIXi6c7a/A8VZuoBaw9m9tdhD88nR/7GG7oRWMVub4oY7_2BO/OtqOu0B56I1LS_2FdHx85_/2FJqjErmgnBnc/fR5wyLVd/zR03KdsDmrJhOpNTELG8Ap7/tRbeA0rm1D/Ahqeb_2B_2Fx66NAH/sAJz2fkfv30m/_2B2yXv1C0u/OTAlb_2Bjz3Xu9/n7nMr5QIveWoLOKJgWpZZ/FZTPBpvOXNqs9vrA/ayBpSg1Jbp3hq/vUJdeVU7/u.jlk	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://94.103	server.exe, 00000000.00000002.569377745.00000000027FC000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.173.142.51	unknown	Russian Federation		34300	SPACENET-ASInternetServiceProviderRU	true
94.103.183.153	unknown	Russian Federation		197390	RATELE-ASRU	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	826138
Start date and time:	2023-03-14 12:25:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 59s
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: 69.7% (good quality ratio 67.8%) • Quality average: 82.1% • Quality standard deviation: 26.5%
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, 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 NtProtectVirtualMemory 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):	6.726307472466791
TrID:	• Win32 Executable (generic) a (10002005/4) 91.23% • Win32 Executable Borland Delphi 7 (665061/41) 6.07% • Win32 Executable Borland Delphi 6 (262906/60) 2.40% • Win32 Executable Delphi generic (14689/80) 0.13% • Windows Screen Saver (13104/52) 0.12%
File name:	server.exe
File size:	616960
MD5:	43cfce2e126b1bf5230e51edd205f6bd
SHA1:	9ca60bfc3cb13b40f02810869ce9531cb0ab76d4
SHA256:	47d288233a39a68396567e35a77a500e296218df3a4bc9daca797e75b4b03d4b
SHA512:	72f203491fab6d44c9f2466b877af56929ba8f24b136b2b706265605e529774efa82bc97b6967791a5d6cd294712667b9a470e543051caa10beb3a73bbab7b78
SSDEEP:	12288:pAP6umkdcE8lZqRpTy2TTHoKKob0xW7//PExk+eVPeYm:Ky0H8lZqRZy4IsHMpeVPq
TLSH:	2FD46C23A2F14437D17717789C7B9766583ABE102E38A88A2BE42D4C4F3D69139753E3
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x476dac
Entrypoint Section:	CODE
Digitally signed:	false

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c180eab77990cded75f412955c2aa3af

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFECh
xor eax, eax
mov dword ptr [ebp-14h], eax
mov eax, 00476AFCh
call 00007F7CFCA5A25Ch
xor eax, eax
push ebp
push 00476E2Dh
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
mov eax, dword ptr [00478AACh]
mov eax, dword ptr [eax]
call 00007F7CFCAAE50Eh
lea edx, dword ptr [ebp-14h]
mov eax, dword ptr [00478AACh]
mov eax, dword ptr [eax]
call 00007F7CFCAAEBA7h
mov eax, dword ptr [ebp-14h]
cmp byte ptr [eax+03h], 0000006Dh
je 00007F7CFCACAB1Ah
mov ecx, dword ptr [00478C4Ch]
mov eax, dword ptr [00478AACh]
mov eax, dword ptr [eax]
mov edx, dword ptr [004762D4h]
call 00007F7CFCAAE4F6h
mov eax, dword ptr [00478AACh]
mov eax, dword ptr [eax]
call 00007F7CFCAAE56Ah
xor eax, eax
pop edx
pop ecx
pop ecx
mov dword ptr fs:[eax], edx
push 00476E34h
lea eax, dword ptr [ebp-14h]
call 00007F7CFCA57E71h
ret
jmp 00007F7CFCA577EBh
jmp 00007F7CFCACAAF2h
call 00007F7CFCA57CF0h
lea eax, dword ptr [eax+00h]

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7a000	0x22ea	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x89000	0x12e00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7f000	0x93a8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x7e000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
CODE	0x1000	0x75e3c	0x76000	False	0.5166139764300848	data	6.558727650455389	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0x77000	0x1d48	0x1e00	False	0.42109375	data	4.29996788400184	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0x79000	0xcd9	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0x7a000	0x22ea	0x2400	False	0.3569878472222222	data	4.9532912812050425	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x7d000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x7e000	0x18	0x200	False	0.048828125	data	0.2005819074398449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x7f000	0x93a8	0x9400	False	0.5329919763513513	data	6.614677812315155	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x12e00	0x12e00	False	0.6307300289735099	data	6.594926097852816	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x89d20	0x134	Targa image data - Map 64 x 65536 x 1 +32 "\001"		
RT_CURSOR	0x89e54	0x134	data		
RT_CURSOR	0x89f88	0x134	data		
RT_CURSOR	0x8a0bc	0x134	data		
RT_CURSOR	0x8a1f0	0x134	data		
RT_CURSOR	0x8a324	0x134	data		
RT_CURSOR	0x8a458	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"		
RT_BITMAP	0x8a58c	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8a75c	0x1e4	Device independent bitmap graphic, 36 x 19 x 4, image size 380		
RT_BITMAP	0x8a940	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8ab10	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8ace0	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8aeb0	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8b080	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8b250	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8b420	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8b5f0	0x1d0	Device independent bitmap graphic, 36 x 18 x 4, image size 360		
RT_BITMAP	0x8b7c0	0xe8	Device independent bitmap graphic, 16 x 16 x 4, image size 128		
RT_ICON	0x8b8a8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_DIALOG	0x8bb90	0x52	data		
RT_STRING	0x8bbe4	0xec	data		
RT_STRING	0x8bcd0	0x42c	data		
RT_STRING	0x8c0fc	0x434	data		
RT_STRING	0x8c530	0x330	data		
RT_STRING	0x8c860	0x4cc	data		
RT_STRING	0x8cd2c	0x3e4	data		
RT_STRING	0x8d110	0x388	data		
RT_STRING	0x8d498	0x440	data		
RT_STRING	0x8d8d8	0x554	data		
RT_STRING	0x8de2c	0x434	data		
RT_STRING	0x8e260	0x510	data		
RT_STRING	0x8e770	0x1e4	data		
RT_STRING	0x8e954	0x1a4	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x8eaf8	0x11c	data		
RT_STRING	0x8ec14	0x2b8	data		
RT_STRING	0x8eecc	0xe0	data		
RT_STRING	0x8efac	0x12c	data		
RT_STRING	0x8f0d8	0x290	data		
RT_STRING	0x8f368	0x40c	data		
RT_STRING	0x8f774	0x37c	data		
RT_STRING	0x8faf0	0x3d4	data		
RT_STRING	0x8fec4	0x250	data		
RT_STRING	0x90114	0xec	data		
RT_STRING	0x90200	0x1dc	data		
RT_STRING	0x903dc	0x3ec	data		
RT_STRING	0x907c8	0x3f4	data		
RT_STRING	0x90bbc	0x30c	data		
RT_STRING	0x90ec8	0x328	data		
RT_RCDATA	0x911f0	0xa604	data	English	United States
RT_RCDATA	0x9b7f4	0x10	data		
RT_RCDATA	0x9b804	0x394	data		
RT_RCDATA	0x9bb98	0x18d	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0x9bd28	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9bd3c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9bd50	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9bd64	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9bd78	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9bd8c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9bda0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x9bdb4	0x14	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, ExitThread, CreateThread, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResumeThread, ResetEvent, ReleaseMutex, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetExitCodeThread, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedIncrement, InterlockedExchange, InterlockedDecrement, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StrokePath, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt

DLL	Import
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MsgWaitForMultipleObjects, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharLowerA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoUninitialize, CoInitialize
oleaut32.dll	GetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
shell32.dll	ShellExecuteExA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

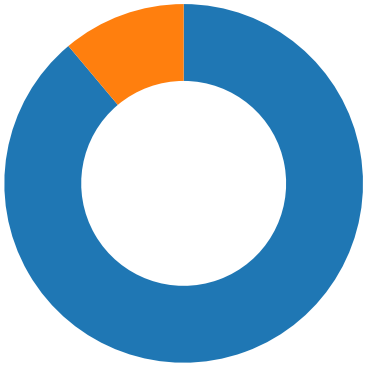
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.462.173.142.51 49685802033203 03/14/23-12:27:29.882824	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49685	80	192.168.2.4	62.173.142.51

Network Port Distribution

Total Packets: 9

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 14, 2023 12:27:29.824017048 CET	49685	80	192.168.2.4	62.173.142.51
Mar 14, 2023 12:27:29.882249117 CET	80	49685	62.173.142.51	192.168.2.4
Mar 14, 2023 12:27:29.882410049 CET	49685	80	192.168.2.4	62.173.142.51
Mar 14, 2023 12:27:29.882823944 CET	49685	80	192.168.2.4	62.173.142.51
Mar 14, 2023 12:27:29.941139936 CET	80	49685	62.173.142.51	192.168.2.4
Mar 14, 2023 12:27:29.941441059 CET	80	49685	62.173.142.51	192.168.2.4
Mar 14, 2023 12:27:29.941647053 CET	49685	80	192.168.2.4	62.173.142.51
Mar 14, 2023 12:27:29.944274902 CET	49685	80	192.168.2.4	62.173.142.51
Mar 14, 2023 12:27:30.002386093 CET	80	49685	62.173.142.51	192.168.2.4
Mar 14, 2023 12:27:49.975713015 CET	49686	80	192.168.2.4	94.103.183.153
Mar 14, 2023 12:27:52.990417957 CET	49686	80	192.168.2.4	94.103.183.153
Mar 14, 2023 12:27:58.994245052 CET	49686	80	192.168.2.4	94.103.183.153

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 14, 2023 12:26:09.669512987 CET	62577	53	192.168.2.4	8.8.8.8
Mar 14, 2023 12:26:09.698645115 CET	53	62577	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 14, 2023 12:26:09.669512987 CET	192.168.2.4	8.8.8.8	0x83d8	Standard query (0)	checklist.skype.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 14, 2023 12:26:09.698645115 CET	8.8.8.8	192.168.2.4	0x83d8	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 62.173.142.51

Statistics

No statistics

System Behavior

Analysis Process: server.exe PID: 5596, Parent PID: 3528

General

Target ID:	0
Start time:	12:26:00
Start date:	14/03/2023
Path:	C:\Users\user\Desktop\server.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\server.exe
Imagebase:	0x400000
File size:	616960 bytes
MD5 hash:	43CFCE2E126B1BF5230E51EDD205F6BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000000.00000002.569302533.0000000002190000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.446824514.00000000035B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.446824514.00000000035B8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.446824514.00000000035B8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.569534669.00000000035B8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.569534669.00000000035B8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.569534669.00000000035B8000.00000004.00000020.00020000.00000000.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