

JOESandbox Cloud BASIC



ID: 830504

Sample Name: server.exe

Cookbook: default.jbs

Time: 12:52:20

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	6
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	6
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	10
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	14
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	18





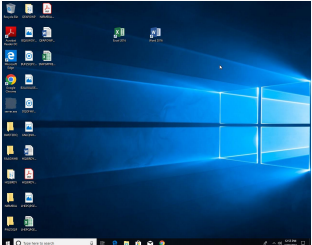
DNS Queries	18
DNS Answers	18
HTTP Request Dependency Graph	19
Statistics	19
System Behavior	19
Analysis Process: server.exePID: 1668, Parent PID: 3452	19
General	19
File Activities	20
Disassembly	20

Windows Analysis Report

server.exe

Overview

General Information

Sample Name:	server.exe
Analysis ID:	830504
MD5:	7e7372ed34c7...
SHA1:	5825f7a627210..
SHA256:	0fa7c98d793b8..
Tags:	agenziaentrate exe gozi isfb ITA mef mise ursnif
Infos:	    
	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

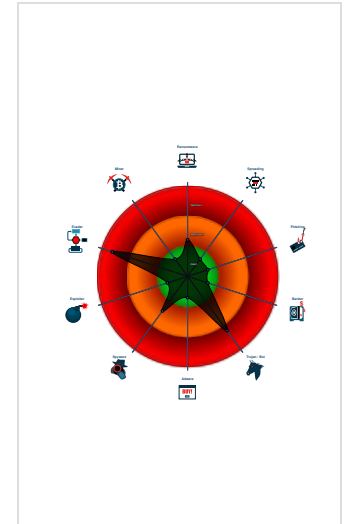
Ursnif

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


Signatures

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

Classification



Process Tree

- System is w10x64
-  server.exe (PID: 1668 cmdline: C:\Users\user\Desktop\server.exe MD5: 7E7372ED34C76CBECA4461BD6DBBF62)
- 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.html http://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-dance https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007	http://https://malpedia.caad.fkie.fr/aunhofer.de/details/win.gozi

Malware Configuration

Threatname: Ursnif

```

{
  "RSA Public Key":
  "ScCjtIu/chsReaToemavuPsGfYIczuvCBcLhySG8/AhfuJmnavu4hmaBPIAXScU9/secJMcCpqdSyeayd2fJdEc3ETZJfeY5SSskXGIyxn6sJL8WH2YF95Gitv+tns2epRbd8/snxdFtGg4Pgf9kxQsW/ySpD96hQxLGzGgDap59E
54E54SLEBTqihX3FWN2//mDaDIJuoFz7lt0whvCg/BgXPBf/s2nkXoRwyyqXguvwDcw9IZEu1NT1qqIwpXL9DGLdaMvfwXTGOLIkQX35RsJJDP1V5Mcgc+c1nBRPKqGQz+NuTKDBIyp0RXXMK3jddMGWvmlL80kvMkvsD8fQxtWRcZ7D
CuQwrQxkXo=",
  "c2_domain": [
    "checkList.skype.com",
    "62.173.142.81",
    "193.233.175.113",
    "109.248.11.184",
    "212.109.218.26",
    "185.68.93.7"
  ],
  "botnet": "7715",
  "server": "50",
  "serpent_key": "xeLJj1BwSDpjfH",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}

```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.437952663.000000002D28000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.437952663.000000002D28000.0000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	<ul style="list-style-type: none"> 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
00000000.00000003.437952663.000000002D28000.0000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	<ul style="list-style-type: none"> 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%u) 0xd96:\$a9: Software\AppDataLow\Software\Microsoft\ 0x1cc0:\$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.437797687.000000002D28000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.437797687.000000002D28000.0000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	<ul style="list-style-type: none"> 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

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: 192.168.2.3 - Destination IP: 62.173.142.81

Timestamp:	192.168.2.362.173.142.8149699802033204 03/20/23-12:55:03.486730
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: 192.168.2.3 - Destination IP: 62.173.142.81

Timestamp:	192.168.2.362.173.142.8149699802033203 03/20/23-12:55:03.486730
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 (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection



Yara detected Ursnif

Malware Analysis System Evasion



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

Anti Debugging



Found API chain indicative of debugger detection

Stealing of Sensitive Information



Yara detected Ursnif

Remote Access Functionality

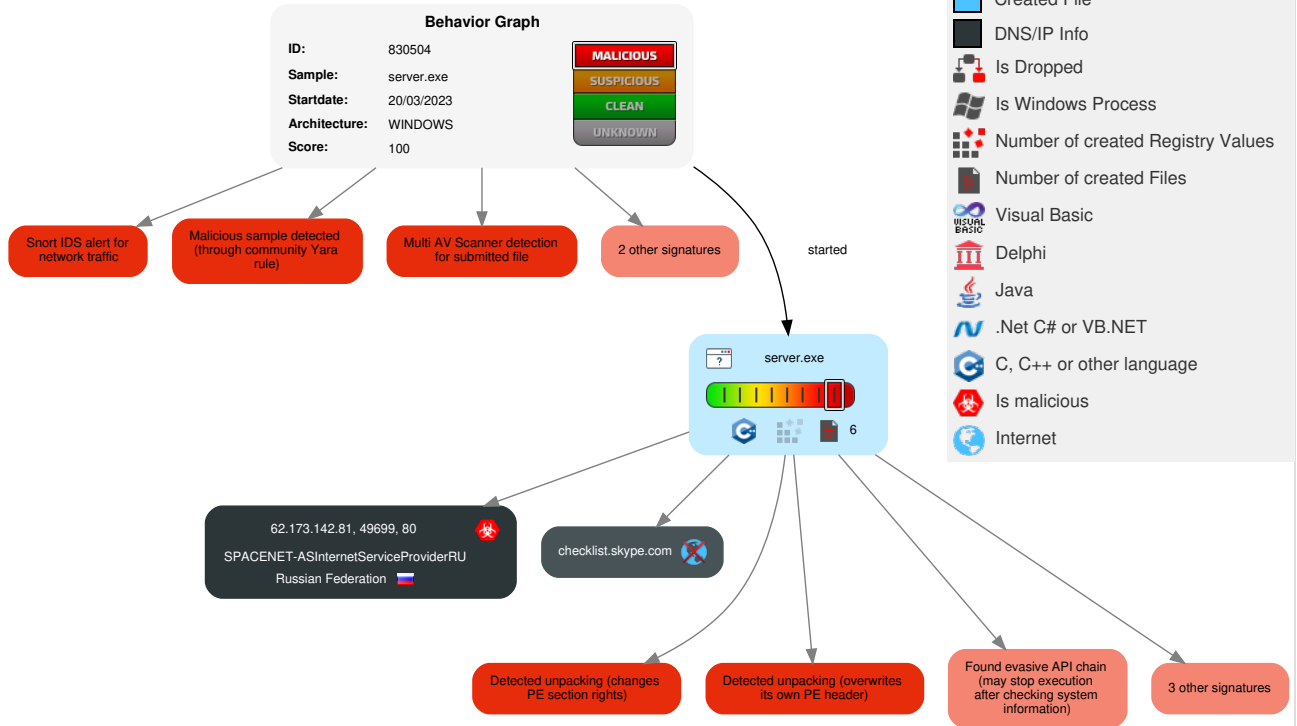


Yara detected Ursnif

Mitre Att&ck Matrix

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

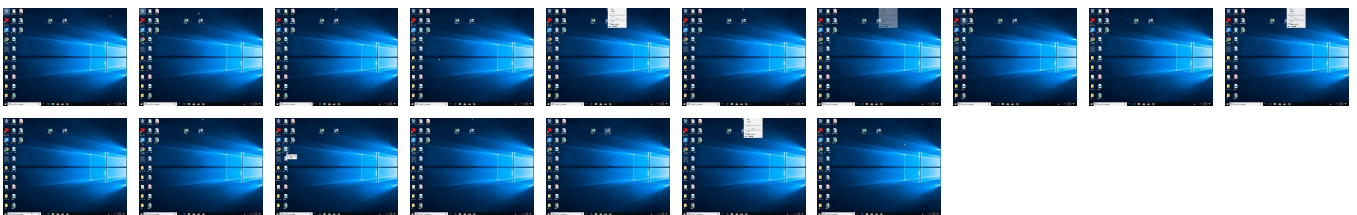
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
server.exe	33%	ReversingLabs		
server.exe	46%	Virustotal		Browse
server.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.server.exe.790000.2.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
0.2.server.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPAC K.Gen7		Download File

Domains

No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://62.173.142.81/drew/jYbXWzWzJZxMu/0bg7r4Fu/6FNvR8ClwgmU3K9eRFHwCZL/V4EUt2dyR_/2FQuIKxQ_2Fze8eK3/SMO5YI_2BPuQ/_2B49snui7_/2FLOe3Ko6as8fp/MUGDOSfZU6Dpa117o0j5G/VqQD_2Bumqn4Myfm/_2BQL_2BhR1HszY/TocLn3p8sVmtowm_2B/6OTZGgFfO/9qQJL2OyxO9xGC6r3J84/1Hw_2BXN3URNn_2FRiR/XmeYSNTVgprtLxVnjmtt4h/zq1_2FWGL3ouV/wUq7EqUY/xzZwPH0P8XChht1uIV1_2F/xZqgBgTuj5/XO.jlk	0%	Avira URL Cloud	safe	
http://62.173.142.81/	0%	Avira URL Cloud	safe	
http://62.173.142.81/drew/jYbXWzWzJZxMu/0bg7r4Fu/6FNvR8ClwgmU3K9eRFHwCZL/V4EUt2dyR_/2FQuIKxQ_2Fze8eK	0%	Avira URL Cloud	safe	
http://62.173	0%	Virustotal		Browse
http://62.173.142.81/	3%	Virustotal		Browse
http://62.173	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://62.173.142.81/drew/jYbXWzWzJZxMu/0bg7r4Fu/6FNvR8ClwgmU3K9eRFHwCZL/V4EUt2dyR_/2FQuIKxQ_2Fze8eK3/SMO5YI_2BPuQ/_2B49snui7_/2FLOe3Ko6as8fp/MUGDOSfZU6Dpa117o0j5G/VqQD_2Bumqn4Myfm/_2BQL_2BhR1HszY/TocLn3p8sVmtowm_2B/6OTZGgFfO/9qQJL2OyxO9xGC6r3J84/1Hw_2BXN3URNn_2FRiR/XmeYSNTVgprtLxVnjmtt4h/zq1_2FWGL3ouV/wUq7EqUY/xzZwPH0P8XChht1uIV1_2F/xZqgBgTuj5/XO.jlk	true	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://checklist.skype.com/drew/atXnm1oMbB5L4NtI5FgyfO/iEVsIQ74abg_2/FW6J1whk/ejMAXerGRdbDd_2FJU9B8H	server.exe, 00000000.00000002.523636233.000000000846000.00000004.00000020.0002000.00000000.sdmp	false		high
http://62.173.142.81/drew/jYbXWzWzJZxMu/0bg7r4Fu/6FNvR8ClwgmU3K9eRFHwCZL/V4EUt2dyR_/2FQuIKxQ_2Fze8eK	server.exe, 00000000.00000002.523636233.000000000873000.00000004.00000020.0002000.00000000.sdmp	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown
http://62.173.142.81/	server.exe, 00000000.00000002.523636233.000000000873000.00000004.00000020.0002000.00000000.sdmp, server.exe, 00000000.00000002.523636233.000000000846000.00000004.00000020.0002000.00000000.sdmp	false	<ul style="list-style-type: none"> 3%, Virustotal, Browse Avira URL Cloud: safe 	unknown
http://62.173	server.exe, 00000000.00000002.523884713.00000000285C000.00000004.00000010.0002000.00000000.sdmp	false	<ul style="list-style-type: none"> 0%, Virustotal, Browse Avira URL Cloud: safe 	low
http://checklist.skype.com/	server.exe, 00000000.00000002.523636233.000000000846000.00000004.00000020.0002000.00000000.sdmp	false		high
http://checklist.skype.com/drew/atXnm1oMbB5L4NtI5Fgy	server.exe, 00000000.00000002.523636233.000000000873000.00000004.00000020.0002000.00000000.sdmp	false		high

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

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830504
Start date and time:	2023-03-20 12:52:20 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	server.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@1/0@1/1
EGA Information:	<ul style="list-style-type: none"> • Successful, ratio: 100%
HDC Information:	<ul style="list-style-type: none"> • Successful, ratio: 53.3% (good quality ratio 51.9%) • Quality average: 82.1% • Quality standard deviation: 26.5%


HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes were 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):	6.799237390766865
TrID:	<ul style="list-style-type: none"> • 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:	181248
MD5:	7e7372ed34c76cbeca4461bd6dbbf62
SHA1:	5825f7a6272108b061a557171da9b8ef6b780028
SHA256:	0fa7c98d793b8c71d6ba29bde4fd449e497b246f92ab30403330fae3d8cb6ffd
SHA512:	2548449b2e5e623600ab080a8213df3164bee0fa9e4690a31c8aac45f856fb7a786dbfc5150202757fe3512ad0d25afc8f635ba67ab08f778c51a9ebb461e284
SSDEEP:	3072:iN5tPqyTcVsXaHJNM1NjtJMD1U85En8d/LZM:MiQPaHihCm85En81Z
TLSH:	2C049EC3A3907865F0158A368E2EC1F4670DF9D2CE59AB66E3186F2F48BC1A2D563711
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.f.Q.f.Q...Q.f.Q..4Q.f.Q...Q.f.Q..9Q.f.Q.f.Q...Q.f.Q..0Q.f.Q..7Q.f.QRich.f.Q.....PE..L...b.b.....

File Icon	
	
Icon Hash:	9a821a4a8592a282

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:	0x62DB62AE [Sat Jul 23 02:53:34 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	2bf4bd16bd9a3948cc472dde1e8c8ccd

Entrypoint Preview	
Instruction	
call 00007FF65CB75C00h	
jmp 00007FF65CB7322Eh	
mov eax, 0040D008h	
ret	
mov eax, dword ptr [0049D540h]	
push esi	
push 00000014h	
pop esi	
test eax, eax	
jne 00007FF65CB733A9h	
mov eax, 00000200h	
jmp 00007FF65CB733A8h	
cmp eax, esi	
jnl 00007FF65CB733A9h	
mov eax, esi	
mov dword ptr [0049D540h], eax	
push 00000004h	
push eax	
call 00007FF65CB75CAEh	
pop ecx	
pop ecx	

Instruction
mov dword ptr [0049C520h], eax
test eax, eax
jne 00007FF65CB733C0h
push 00000004h
push esi
mov dword ptr [0049D540h], esi
call 00007FF65CB75C95h
pop ecx
pop ecx
mov dword ptr [0049C520h], eax
test eax, eax
jne 00007FF65CB733A7h
push 0000001Ah
pop eax
pop esi
ret
xor edx, edx
mov ecx, 0040D008h
jmp 00007FF65CB733A7h
mov eax, dword ptr [0049C520h]
mov dword ptr [edx+eax], ecx
add ecx, 20h
add edx, 04h
cmp ecx, 0040D288h
jl 00007FF65CB7338Ch
push FFFFFFFEh
pop esi
xor edx, edx
mov ecx, 0040D018h
push edi
mov eax, edx
sar eax, 05h
mov eax, dword ptr [0049C420h+eax*4]
mov edi, edx
and edi, 1Fh
shl edi, 06h
mov eax, dword ptr [edi+eax]
cmp eax, FFFFFFFFh
je 00007FF65CB733AAh
cmp eax, esi
je 00007FF65CB733A6h
test eax, eax
jne 00007FF65CB733A4h
mov dword ptr [ecx], esi
add ecx, 20h
inc edx
cmp ecx, 0040D078h
jl 00007FF65CB73370h
pop edi
xor eax, eax
pop esi
ret
call 00007FF65CB739B6h
cmp byte ptr [00000000h], 00000000h

Rich Headers

Programming Language:	<ul style="list-style-type: none"> [C++] VS2010 build 30319 [ASM] VS2010 build 30319 [C] VS2010 build 30319 [IMP] VS2008 SP1 build 30729 [RES] VS2010 build 30319 [LNK] VS2010 build 30319
-----------------------	--

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb84c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9f000	0xdaf0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2b08	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x19c	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb1ae	0xb200	False	0.5147033005617978	data	6.020837660539205	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xd000	0x9054c	0x13000	False	0.9465589021381579	data	7.853280851360385	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.xresof	0x9e000	0x96	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x9f000	0xdaf0	0xdc00	False	0.41329900568181815	data	4.474423213582852	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ



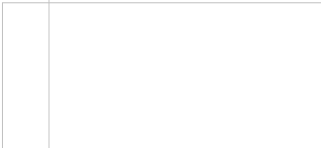
Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0xab598	0x2	data		
TONIZITOWAPEVUMOBEM	0xaaea0	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Finland
TONIZITOWAPEVUMOBEM	0xaaea0	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Norway
TONIZITOWAPEVUMOBEM	0xaaea0	0x598	ASCII text, with very long lines (1432), with no line terminators	Sami Lappish	Sweden
RT_CURSOR	0xab5a0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xab6d0	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0xab7c0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x9f680	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0x9f680	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0x9f680	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0x9ff28	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0x9ff28	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway

Name	RVA	Size	Type	Language	Country
RT_ICON	0x9ff28	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa0ff8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa0ff8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa0ff8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa18a0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa18a0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa18a0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa3e48	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa3e48	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa3e48	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa4f20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa4f20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa4f20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa5dc8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa5dc8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa5dc8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa6490	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xa6490	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xa6490	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xa69f8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa69f8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa69f8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xa8fa0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xa8fa0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xa8fa0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xaa048	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xaa048	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xaa048	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xaa9d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xaa9d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xaa9d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Sweden
RT_ACCELERATOR	0xab4e0	0x78	data	Sami Lappish	Finland
RT_ACCELERATOR	0xab4e0	0x78	data	Sami Lappish	Norway
RT_ACCELERATOR	0xab4e0	0x78	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xab438	0xa8	data	Sami Lappish	Finland
RT_ACCELERATOR	0xab438	0xa8	data	Sami Lappish	Norway
RT_ACCELERATOR	0xab438	0xa8	data	Sami Lappish	Sweden
RT_GROUP_CURSOR	0xac868	0x30	data		

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0xa4ef0	0x30	data	Sami Lappish	Finland
RT_GROUP_ICON	0xa4ef0	0x30	data	Sami Lappish	Norway
RT_GROUP_ICON	0xa4ef0	0x30	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xa0fd0	0x22	data	Sami Lappish	Finland
RT_GROUP_ICON	0xa0fd0	0x22	data	Sami Lappish	Norway
RT_GROUP_ICON	0xa0fd0	0x22	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xaae38	0x68	data	Sami Lappish	Finland
RT_GROUP_ICON	0xaae38	0x68	data	Sami Lappish	Norway
RT_GROUP_ICON	0xaae38	0x68	data	Sami Lappish	Sweden
RT_VERSION	0xac898	0x258	data		
None	0xab558	0xa	data	Sami Lappish	Finland
None	0xab558	0xa	data	Sami Lappish	Norway
None	0xab558	0xa	data	Sami Lappish	Sweden
None	0xab568	0xa	data	Sami Lappish	Finland
None	0xab568	0xa	data	Sami Lappish	Norway
None	0xab568	0xa	data	Sami Lappish	Sweden
None	0xab578	0xa	data	Sami Lappish	Finland
None	0xab578	0xa	data	Sami Lappish	Norway
None	0xab578	0xa	data	Sami Lappish	Sweden
None	0xab588	0xa	data	Sami Lappish	Finland
None	0xab588	0xa	data	Sami Lappish	Norway
None	0xab588	0xa	data	Sami Lappish	Sweden

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

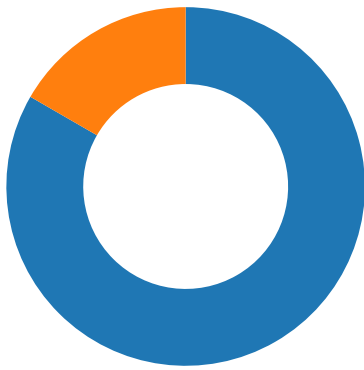
Possible Origin		
Language of compilation system	Country where language is spoken	Map
Sami Lappish	Finland	
Sami Lappish	Norway	
Sami Lappish	Sweden	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.362.173.142.81 49699802033204 03/20/23- 12:55:03.486730	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49699	80	192.168.2.3	62.173.142.81
192.168.2.362.173.142.81 49699802033203 03/20/23- 12:55:03.486730	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49699	80	192.168.2.3	62.173.142.81

Network Port Distribution



Total Packets: 6

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 12:55:03.422652960 CET	49699	80	192.168.2.3	62.173.142.81
Mar 20, 2023 12:55:03.486253023 CET	80	49699	62.173.142.81	192.168.2.3
Mar 20, 2023 12:55:03.486366034 CET	49699	80	192.168.2.3	62.173.142.81
Mar 20, 2023 12:55:03.486730099 CET	49699	80	192.168.2.3	62.173.142.81
Mar 20, 2023 12:55:03.549804926 CET	80	49699	62.173.142.81	192.168.2.3
Mar 20, 2023 12:55:03.550898075 CET	80	49699	62.173.142.81	192.168.2.3
Mar 20, 2023 12:55:03.551032066 CET	49699	80	192.168.2.3	62.173.142.81
Mar 20, 2023 12:55:03.553265095 CET	49699	80	192.168.2.3	62.173.142.81
Mar 20, 2023 12:55:03.616254091 CET	80	49699	62.173.142.81	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 12:53:43.233784914 CET	62704	53	192.168.2.3	8.8.8.8
Mar 20, 2023 12:53:43.259754896 CET	53	62704	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 12:53:43.233784914 CET	192.168.2.3	8.8.8.8	0xcfa8	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 12:53:43.259754896 CET	8.8.8.8	192.168.2.3	0xcfa8	Name error (3)	checklist. skype.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 62.173.142.81

Statistics

 No statistics

System Behavior


Analysis Process: server.exe PID: 1668, Parent PID: 3452

General

Target ID:	0
Start time:	12:53:17
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:	181248 bytes
MD5 hash:	7E7372ED34C76CBECA4461BD6DBBF62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	<ul style="list-style-type: none"> • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437952663.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437952663.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437952663.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437797687.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437797687.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437797687.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437940393.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437940393.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437940393.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.523539634.000000000816000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437762221.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.523315446.000000000610000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437762221.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437762221.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437924768.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437924768.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437924768.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.523909474.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.523909474.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.523909474.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437846787.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437846787.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437846787.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437887198.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437887198.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437887198.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.437824443.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.437824443.0000000002D28000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.437824443.0000000002D28000.00000004.00000020.00020000.00000000.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	