ID: 826246
Sample Name:
KOYCdGz80D.exe
Cookbook: default.jbs
Time: 14:58:14
Date: 14/03/2023
Version: 37.0.0 Beryl

Table of Contents

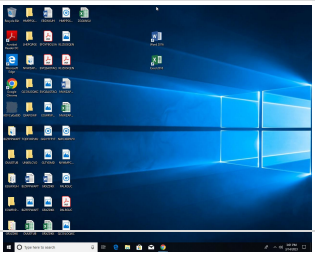
Windows Analysis Report

KOYCdGz80D.exe

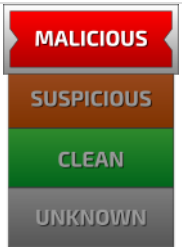
Overview

General Information

Sample Name:	KOYCdGz80D.exe
Original Sample Name:	d09f787a952a6..
Analysis ID:	826246
MD5:	d09f787a952a6..
SHA1:	c3c3cbad8d40…
SHA256:	8cd071a056f55..
Tags:	250255 7713 exe Gozi ISFB Ursnif
Infos:	



Detection



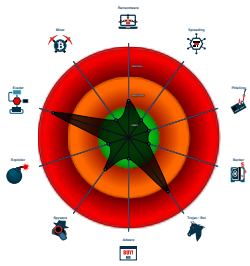
Ursnif

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- KOYCdGz80D.exe (PID: 5348 cmdline: C:\Users\user\Desktop\KOYCdGz80D.exe MD5: D09F787A952A6E946656AC9184768FBE)
- **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
00000000.00000003.418089907.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.418089907.0000000002BE8000.00000004.00000020.00020000.00000000.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:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.418089907.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$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:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.417900586.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.417900586.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$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

Click to see the 27 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 62.173.142.51	
Timestamp:	192.168.2.762.173.142.5149700802033203 03/14/23-15:00:52.733532
SID:	2033203
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.7 - Destination IP: 62.173.142.51	
Timestamp:	192.168.2.762.173.142.5149700802033204 03/14/23-15:00:52.733532
SID:	2033204
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

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

Anti Debugging

Found API chain indicative of debugger detection

Stealing of Sensitive Information

Yara detected Ursnif

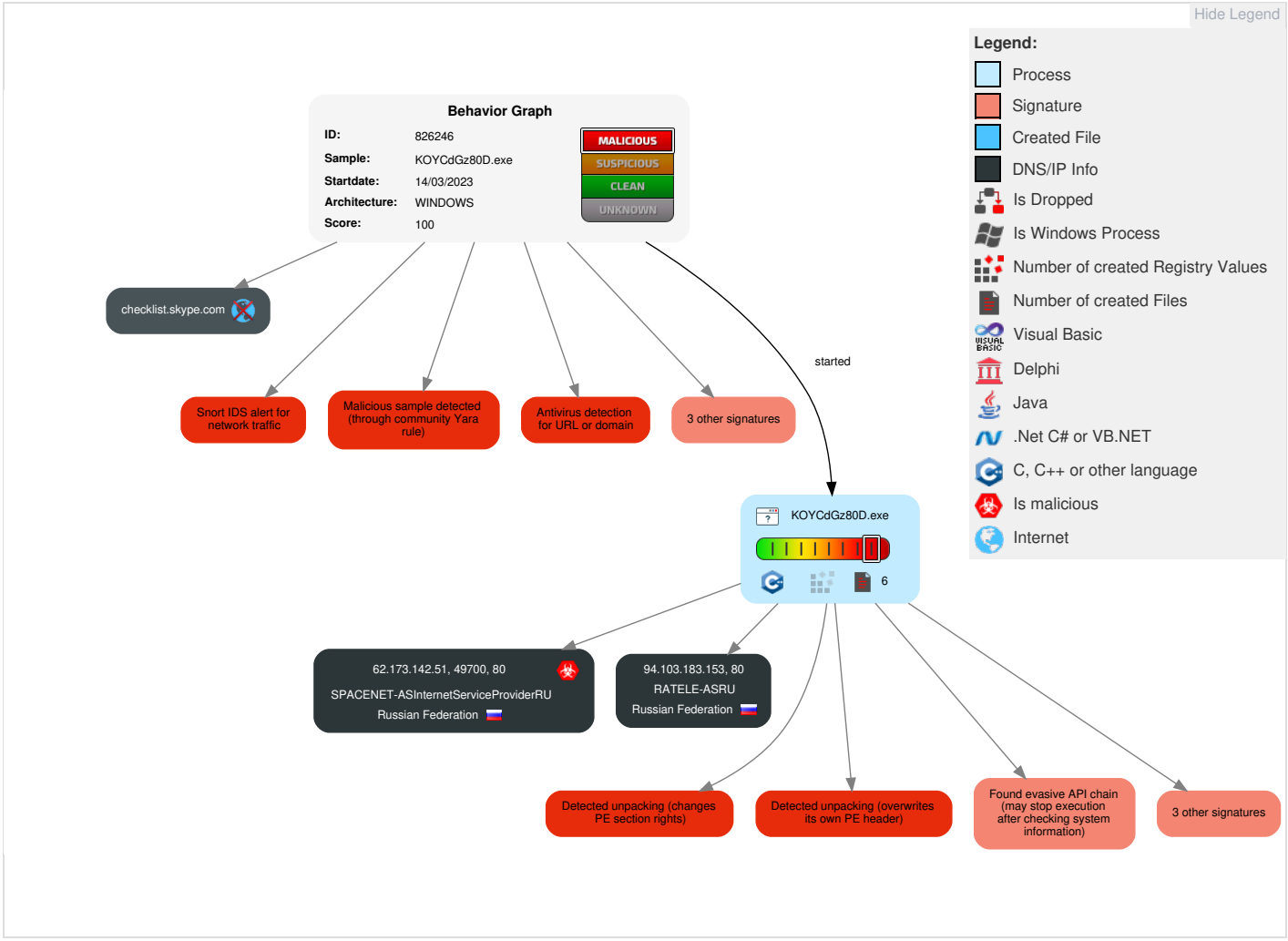
Remote Access Functionality

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Windows Management Instrumentation	Path Interception	Path Interception	1 1 Virtualization/Sandbox Evasion	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	1 Obfuscated Files or Information	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	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 Remote System 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 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
KOYCdGz80D.exe	52%	Virustotal		Browse
KOYCdGz80D.exe	49%	ReversingLabs	Win32.Trojan.Generic	
KOYCdGz80D.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.KOYCdGz80D.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.KOYCdGz80D.exe.640000.2.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://94.103.183.153/ws	100%	Avira URL Cloud	malware	
http://94.103.183.153/drew/ZPHuUA_2/FprSm4ZnZ_2BAzE0dNANwbe/iluX9tql3G/HloTTZMt_2B0yd_2F/E7gfm_2FdCi	100%	Avira URL Cloud	malware	
http://62.173.142.51/drew/nxxSRbXkG/Z9AQFeMulxsZ78vPJ0Ba/xgGOAFgVNpjYUN1Ulcb/8uwliaMwLO1graJYCm8PkM/IU0adVtArkJ_2/BZSxJ28e/Tc5ERYxiq7NBJmMEOo_2FLz/U3IE7OaYn6/s6_2BEZEnVZDoNKzr/yGWuv6V_2Fey/iblrbuFvdzu/G5cNIxcFhMXXH4/DW8BYhEM_2Bfx1WgbZGW2/9wbrpFGQVXKMRqQD/zmPaF1BbhLFtoKq/CFytgFZSMFNAbTktuc/B_2FQe4sV/W6Pv_2BAatm_2Ft2VjTv/WRtPQxXM/lSCDVEp9/l.jlk	100%	Avira URL Cloud	malware	
http://62.173.142.51/drew/nxxSRbXkG/Z9AQFeMulxsZ78vPJ0Ba/xgGOAFgVNpjYUN1Ulcb/8uwliaMwLO1graJYCm8PkM/	100%	Avira URL Cloud	malware	
http://94.103.183.153/	100%	Avira URL Cloud	malware	
http://62.173.142.51/	100%	Avira URL Cloud	malware	
http://94.103	0%	Avira URL Cloud	safe	
http://62.173.142.51/	2%	Virustotal		Browse

Domains and IPs

Contacted Domains

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

Contacted URLs

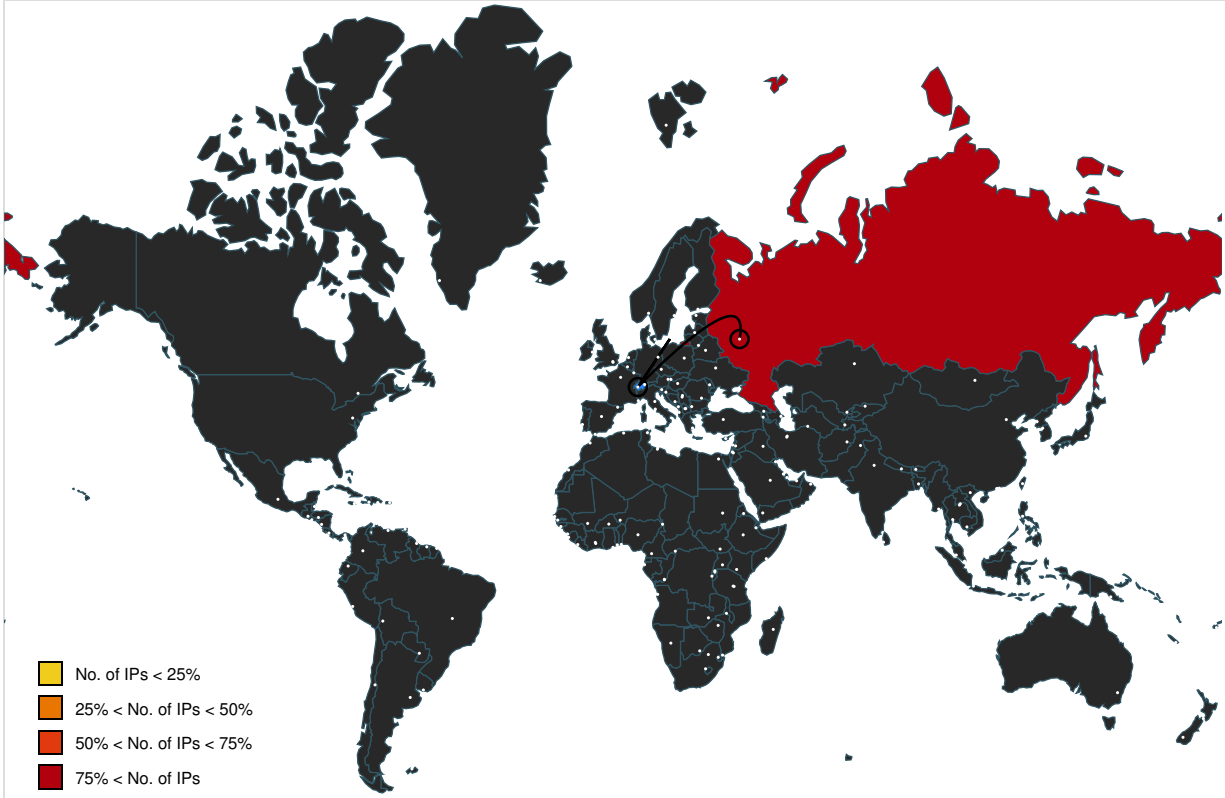
Name	Malicious	Antivirus Detection	Reputation
http://62.173.142.51/drew/nxxSRbXkG/Z9AQFeMulxsZ78vPJ0Ba/xgGOAFgVNpjYUN1Ulcb/8uwliaMwLO1graJYCm8PkM/IU0adVtArkJ_2/BZSxJ28e/Tc5ERYxiq7NBJmMEOo_2FLz/U3IE7OaYn6/s6_2BEZEnVZDoNKzr/yGWuv6V_2Fey/iblrbuFvdzu/G5cNIxcFhMXXH4/DW8BYhEM_2Bfx1WgbZGW2/9wbrpFGQVXKMRqQD/zmPaF1BbhLFtoKq/CFytgFZSMFNAbTktuc/B_2FQe4sV/W6Pv_2BAatm_2Ft2VjTv/WRtPQxXM/lSCDVEp9/l.jlk	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://62.173.142.51/drew/nxxSRbXkG/Z9AQFeMulxsZ78vPJ0Ba/xgGOAFgVNpjYUN1Ulcb/8uwliaMwLO1graJYCm8PkM/	KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000833000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://checklist.skype.com/drew/3PKTGV3tNzaVLTkq/t_2Fk5P4Y6K9Qzr/6RM6HLfcw_2BRzYyd_/2FngDszCZ/8roslt	KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000833000.00000004.00000020.00020000.00000000.sdmp	false		high
http://62.173.142.51/	KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000878000.00000004.00000020.00020000.00000000.sdmp, KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000833000.00000004.00000020.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://94.103.183.153/ws	KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000833000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://94.103.183.153/drew/ZPHuUA_2/FprSm4ZnZ_2BAzE0dNANwbe/iluX9tql3G/HloTTZMt_2B0yd_2F/E7gfm_2FdCi	KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000833000.00000004.00000020.00020000.00000000.sdmp, KOYCdGz80D.exe, 00000000.00000002.509156874.0000000000809000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://checklist.skype.com/6WkbUYRz/dPSG7YZOtAhk9jZCO3f	KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000833000.00000004.00000020.00020000.00000000.sdmp	false		high
http://94.103.183.153/	KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000833000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://94.103	KOYCdGz80D.exe, 00000000.00000002.509470240.000000000229C000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://checklist.skype.com/drew/3PKTGV3tS	KOYCdGz80D.exe, 00000000.00000002.509334762.0000000000833000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

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:	826246
Start date and time:	2023-03-14 14:58:14 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Sample file name:	KOYCdGz80D.exe
Original Sample Name:	d09f787a952a6e946656ac9184768fbe.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@1/0@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 5.2% (good quality ratio 5.2%) • Quality average: 89% • Quality standard deviation: 15.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.825405817982751
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:	KOYCdGz80D.exe
File size:	240128
MD5:	d09f787a952a6e946656ac9184768fbe
SHA1:	c3c3cbad8d40c7ba332c2b6d7ae0464d092c0877
SHA256:	8cd071a056f555c793b95c82f9eff1fcf60e304a1e9589988e9819f27a754256
SHA512:	d99dbae675932c18280103de4553777aaebe051a6da11a651a665a34c5bdf3aef2b97f1ab8195d652572b6a7e9ae9547fc583b9e666c1ee9715561f3fd2af345
SSDEEP:	3072:T1rxrNcNq2GawilCy9y1UKk4BauPffL1xrN2fKdGJh0RxW2NM6BoaM6:LNyqAwgCQmouPnL1xN2kQ2NMioa
TLSH:	00348E1272D0A871E7324631BE2BD3B5661EFCA18F5D6AEB23846A2F4D711E1CE71341
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....aBL...L...L...#...\...#.../...E...G...L...:...#...a...#...M...#...M...RichL.....PE..L...;c5b.....

File Icon

Icon Hash:	9a82024281828a84

Static PE Info

General

Entrypoint:	0x409761
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:	0x6235633B [Sat Mar 19 04:59:39 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:	ae274c29ca15928cb1e23f2e712ba155

Entrypoint Preview

Instruction
call 00007FB2F8A8F4AEh
jmp 00007FB2F8A88ECEh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
test eax, eax
je 00007FB2F8A89054h
sub eax, 08h
cmp dword ptr [eax], 0000DDDDh
jne 00007FB2F8A89049h
push eax

Instruction
call 00007FB2F8A88667h
pop ecx
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007FB2F8A890A5h
call 00007FB2F8A8C01Dh
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [0042D710h]
je 00007FB2F8A89054h
mov ecx, dword ptr [0042D4C8h]
test dword ptr [eax+70h], ecx
jne 00007FB2F8A89049h
call 00007FB2F8A8FE88h
mov dword ptr [esi], eax
mov eax, dword ptr [esi+04h]
cmp eax, dword ptr [0042D3D0h]
je 00007FB2F8A89058h
mov eax, dword ptr [esi+08h]
mov ecx, dword ptr [0042D4C8h]
test dword ptr [eax+70h], ecx
jne 00007FB2F8A8904Ah
call 00007FB2F8A8F6E7h
mov dword ptr [esi+04h], eax
mov eax, dword ptr [esi+08h]
test byte ptr [eax+70h], 00000002h
jne 00007FB2F8A89056h
or dword ptr [eax+70h], 02h
mov byte ptr [esi+0Ch], 00000001h
jmp 00007FB2F8A8904Ch
mov ecx, dword ptr [eax]
mov dword ptr [esi], ecx
mov eax, dword ptr [eax+04h]
mov dword ptr [esi+04h], eax
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 10h
mov eax, dword ptr [0042CCD8h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
mov edx, dword ptr [ebp+18h]
push ebx

Rich Headers

Programming Language:	• [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [C++] VS2010 build 30319 • [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	0x18f6c	0x78	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0xdd08	.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	0x4320	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.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	0x18a14	0x18c00	False	0.5078519570707071	data	6.314209619196138	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x91248	0x13c00	False	0.9314057555379747	data	7.829501179808203	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xac000	0xdd08	0xde00	False	0.40860782657657657	data	4.398436868519861	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xb7f48	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xb8090	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0xb81c0	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0xb82b0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0xac5e0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xac5e0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xac5e0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xace88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xace88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xace88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xadf58	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xadf58	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Norway

Name	RVA	Size	Type	Language	Country
RT_ICON	0xadf58	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xae800	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xae800	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xae800	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb0da8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb0da8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb0da8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb1e80	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xb1e80	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xb1e80	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xb2d28	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xb2d28	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xb2d28	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xb33f0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Finland
RT_ICON	0xb33f0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Norway
RT_ICON	0xb33f0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Sami Lappish	Sweden
RT_ICON	0xb3958	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb3958	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb3958	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb5f00	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb5f00	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb5f00	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb6fa8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb6fa8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb6fa8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Sami Lappish	Sweden
RT_ICON	0xb7930	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Finland
RT_ICON	0xb7930	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Norway
RT_ICON	0xb7930	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Sami Lappish	Sweden
RT_STRING	0xb95d8	0x3be	data	Sami Lappish	Finland
RT_STRING	0xb95d8	0x3be	data	Sami Lappish	Norway
RT_STRING	0xb95d8	0x3be	data	Sami Lappish	Sweden
RT_STRING	0xb9998	0x36a	data	Sami Lappish	Finland
RT_STRING	0xb9998	0x36a	data	Sami Lappish	Norway
RT_STRING	0xb9998	0x36a	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xb7ea8	0x90	data	Sami Lappish	Finland
RT_ACCELERATOR	0xb7ea8	0x90	data	Sami Lappish	Norway
RT_ACCELERATOR	0xb7ea8	0x90	data	Sami Lappish	Sweden
RT_ACCELERATOR	0xb7e00	0xa8	data	Sami Lappish	Finland
RT_ACCELERATOR	0xb7e00	0xa8	data	Sami Lappish	Norway
RT_ACCELERATOR	0xb7e00	0xa8	data	Sami Lappish	Sweden

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0xb8078	0x14	data		
RT_GROUP_CURSOR	0xb9358	0x30	data		
RT_GROUP_ICON	0xb1e50	0x30	data	Sami Lappish	Finland
RT_GROUP_ICON	0xb1e50	0x30	data	Sami Lappish	Norway
RT_GROUP_ICON	0xb1e50	0x30	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xadf30	0x22	data	Sami Lappish	Finland
RT_GROUP_ICON	0xadf30	0x22	data	Sami Lappish	Norway
RT_GROUP_ICON	0xadf30	0x22	data	Sami Lappish	Sweden
RT_GROUP_ICON	0xb7d98	0x68	data	Sami Lappish	Finland
RT_GROUP_ICON	0xb7d98	0x68	data	Sami Lappish	Norway
RT_GROUP_ICON	0xb7d98	0x68	data	Sami Lappish	Sweden
RT_VERSION	0xb9388	0x24c	data		
None	0xb7f38	0xa	data	Sami Lappish	Finland
None	0xb7f38	0xa	data	Sami Lappish	Norway
None	0xb7f38	0xa	data	Sami Lappish	Sweden

Imports

DLL	Import
KERNEL32.dll	PulseEvent, ReadConsoleInputW, GetFirmwareEnvironmentVariableW, GetCPInfoExW, CreateEventW, CopyFileExA, GetProcAddress, GlobalAlloc, SetDefaultCommConfigA, OpenWaitableTimerW, GetFileAttributesW, EnumResourceTypesW, WriteFileGather, GetModuleHandleW, InterlockedCompareExchange, UnhandledExceptionFilter, LocalFlags, GlobalLock, GetConsoleAliasW, WritePrivateProfileSectionA, FindFirstVolumeMountPointA, SetLastError, SleepEx, AddAtomA, lstrcmpA, SetCalendarInfoA, GetSystemWindowsDirectoryA, EnumTimeFormatsW, GetSystemDirectoryW, AddAtomW, GetExitCodeThread, _llseek, FindNextFileW, CopyFileA, GetShortPathNameW, EnumCalendarInfoA, EnumCalendarInfoExA, AddRefActCtx, SetStdHandle, WriteConsoleW, GetCurrentThreadId, LoadLibraryA, CloseHandle, SetFilePointer, ReadFile, FlushFileBuffers, InterlockedIncrement, InterlockedDecrement, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, EncodePointer, DecodePointer, GetLastError, HeapFree, RtlUnwind, RaiseException, HeapReAlloc, HeapAlloc, MoveFileA, DeleteFileA, GetCommandLineA, HeapSetInformation, GetStartupInfoW, WideCharToMultiByte, LCMapStringW, MultiByteToWideChar, GetCPInfo, IsProcessorFeaturePresent, HeapCreate, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameW, SetUnhandledExceptionFilter, IsDebuggerPresent, TerminateProcess, GetCurrentProcess, GetModuleFileNameA, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, InitializeCriticalSectionAndSpinCount, GetFileType, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetACP, GetOEMCP, IsValidCodePage, GetStringTypeW, GetLocaleInfoW, HeapSize, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, LoadLibraryW, GetConsoleCP, GetConsoleMode, CreateFileW
USER32.dll	LoadMenuW
ADVAPI32.dll	LookupAccountSidW
SHELL32.dll	FindExecutableA
ole32.dll	CoGetInstanceFromFile

Possible Origin

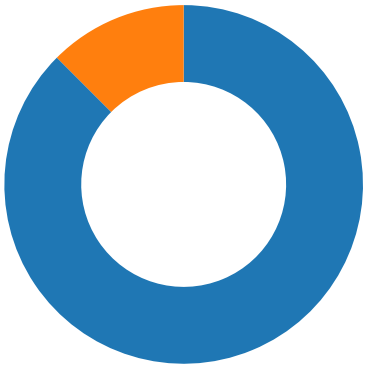
Language of compilation system	Country where language is spoken	Map
Sami Lappish	Finland	
Sami Lappish	Norway	
Sami Lappish	Sweden	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.762.173.142.51 49700802033203 03/14/23-15:00:52.733532	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49700	80	192.168.2.7	62.173.142.51
192.168.2.762.173.142.51 49700802033204 03/14/23-15:00:52.733532	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49700	80	192.168.2.7	62.173.142.51

Network Port Distribution



Total Packets: 8

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 14, 2023 15:00:52.673491001 CET	49700	80	192.168.2.7	62.173.142.51
Mar 14, 2023 15:00:52.732873917 CET	80	49700	62.173.142.51	192.168.2.7
Mar 14, 2023 15:00:52.733180046 CET	49700	80	192.168.2.7	62.173.142.51
Mar 14, 2023 15:00:52.733531952 CET	49700	80	192.168.2.7	62.173.142.51
Mar 14, 2023 15:00:52.793348074 CET	80	49700	62.173.142.51	192.168.2.7
Mar 14, 2023 15:00:52.794256926 CET	80	49700	62.173.142.51	192.168.2.7
Mar 14, 2023 15:00:52.794380903 CET	49700	80	192.168.2.7	62.173.142.51
Mar 14, 2023 15:00:52.803956032 CET	49700	80	192.168.2.7	62.173.142.51
Mar 14, 2023 15:00:52.863280058 CET	80	49700	62.173.142.51	192.168.2.7
Mar 14, 2023 15:01:12.834670067 CET	49701	80	192.168.2.7	94.103.183.153
Mar 14, 2023 15:01:15.835302114 CET	49701	80	192.168.2.7	94.103.183.153

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 14, 2023 14:59:32.458257914 CET	59477	53	192.168.2.7	8.8.8.8
Mar 14, 2023 14:59:32.485673904 CET	53	59477	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 14, 2023 14:59:32.458257914 CET	192.168.2.7	8.8.8.8	0xb87d	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 14:59:32.485673904 CET	8.8.8.8	192.168.2.7	0xb87d	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: KOYCdGz80D.exe PID: 5348, Parent PID: 3320

General

Target ID:	0
Start time:	14:59:10
Start date:	14/03/2023
Path:	C:\Users\user\Desktop\KOYCdGz80D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\KOYCdGz80D.exe
Imagebase:	0x400000
File size:	240128 bytes
MD5 hash:	D09F787A952A6E946656AC9184768FBE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.418089907.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.418089907.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.418089907.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.417900586.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.417900586.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.417900586.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.418062084.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.418062084.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.418062084.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.509300056.0000000000820000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.508996515.0000000000620000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.509844164.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.509844164.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.509844164.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.417978343.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.417978343.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.417978343.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.417934305.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.417934305.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.417934305.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.418044877.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.418044877.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.418044877.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.418004616.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.418004616.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.418004616.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.418106797.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.418106797.0000000002BE8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.418106797.0000000002BE8000.00000004.00000020.00020000.00000000.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