ID: 552763
Sample Name: 3Wok4G7Goe
Cookbook: default.jbs
Time: 17:55:06
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

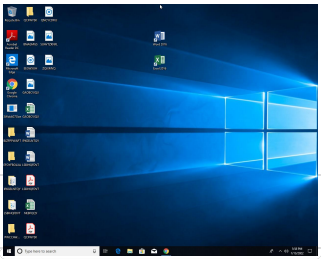
Windows Analysis Report 3Wok4G7Goe

Overview

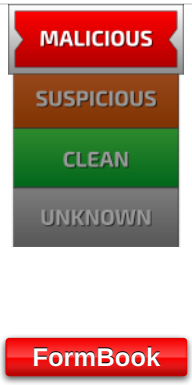
General Information

Sample Name:	3Wok4G7Goe (renamed file extension from none to exe)
Analysis ID:	552763
MD5:	1e14373563bcf10.
SHA1:	f19d6f0a506f860…
SHA256:	8d38be02ab71fba.
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



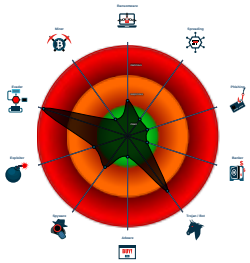
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- 3Wok4G7Goe.exe (PID: 6492 cmdline: "C:\Users\user\Desktop\3Wok4G7Goe.exe" MD5: 1E14373563BCF10103F2850B17B100EA)
  - powershell.exe (PID: 6748 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6784 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\eyFgpnfXIO" /XML "C:\Users\user\AppData\Local\Temp\tmpDDB3.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 3Wok4G7Goe.exe (PID: 6948 cmdline: C:\Users\user\Desktop\3Wok4G7Goe.exe MD5: 1E14373563BCF10103F2850B17B100EA)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - systray.exe (PID: 6552 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.topeasyip.company/i5nb/"
  ],
  "decoy": [
    "integratedheartspsychology.com",
    "tappsis.land",
    "norfg.com",
    "1531700.win",
    "oneplusoneexperience.com",
    "circlessalaries.com",
    "tlcremodelingcompany.com",
    "susalud.info",
    "liyanghua.club",
    "pink-zemi.com",
    "orphe.biz",
    "themodelclarified.com",
    "candidate.tools",
    "morotrip.com",
    "d2dfms.com",
    "leisuresabah.com",
    "bjbwx114.com",
    "lz-fcaini1718-hw0917-bs.xyz",
    "at-commerce-co.net",
    "buymypolicy.net",
    "5151vip73.com",
    "rentglide.com",
    "louiecruzbeltran.info",
    "lanabasargina.com",
    "lakeforestparkapartments.com",
    "guangkaiyinwu.com",
    "bornthin.com",
    "restaurantkitchenbuilders.com",
    "ecommerceoptimise.com",
    "datahk99.com",
    "markfwalker.com",
    "granitowawarszawa.com",
    "theyouthwave.com",
    "iabg.xyz",
    "jholbrook.com",
    "bsc.promo",
    "xn--grlitzerseebhne-8sb7i.com",
    "cafeteriasula.com",
    "plushcrispies.com",
    "dedicatedvirtualassistance.com",
    "ventura-taxi.com",
    "thoethertb434-ocn.xyz",
    "ylhwcl.com",
    "bigsyncmusic.biz",
    "terapiaholisticaemformacao.com",
    "comidies.com",
    "171diproad.com",
    "07dgj.xyz",
    "vppaintllc.com",
    "thepatriottutor.com",
    "wxfive.com",
    "ceinpsico.com",
    "tuningelement.store",
    "asinment.com",
    "diafraz.xyz",
    "8crhnwh658ga.biz",
    "redwolf-tech.com",
    "ksherfan.com",
    "sensationalshroom.com",
    "buy-instagram-followers.net",
    "treeserviceconsulting.com",
    "vnln.space",
    "kate-films.com",
    "selfmeta.club"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.281378639.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.281378639.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000000.281378639.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000012.00000002.514743460.0000000002130000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000012.00000002.514743460.0000000002130000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.3Wok4G7Goe.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.3Wok4G7Goe.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.3Wok4G7Goe.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
7.0.3Wok4G7Goe.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.0.3Wok4G7Goe.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected FormBook

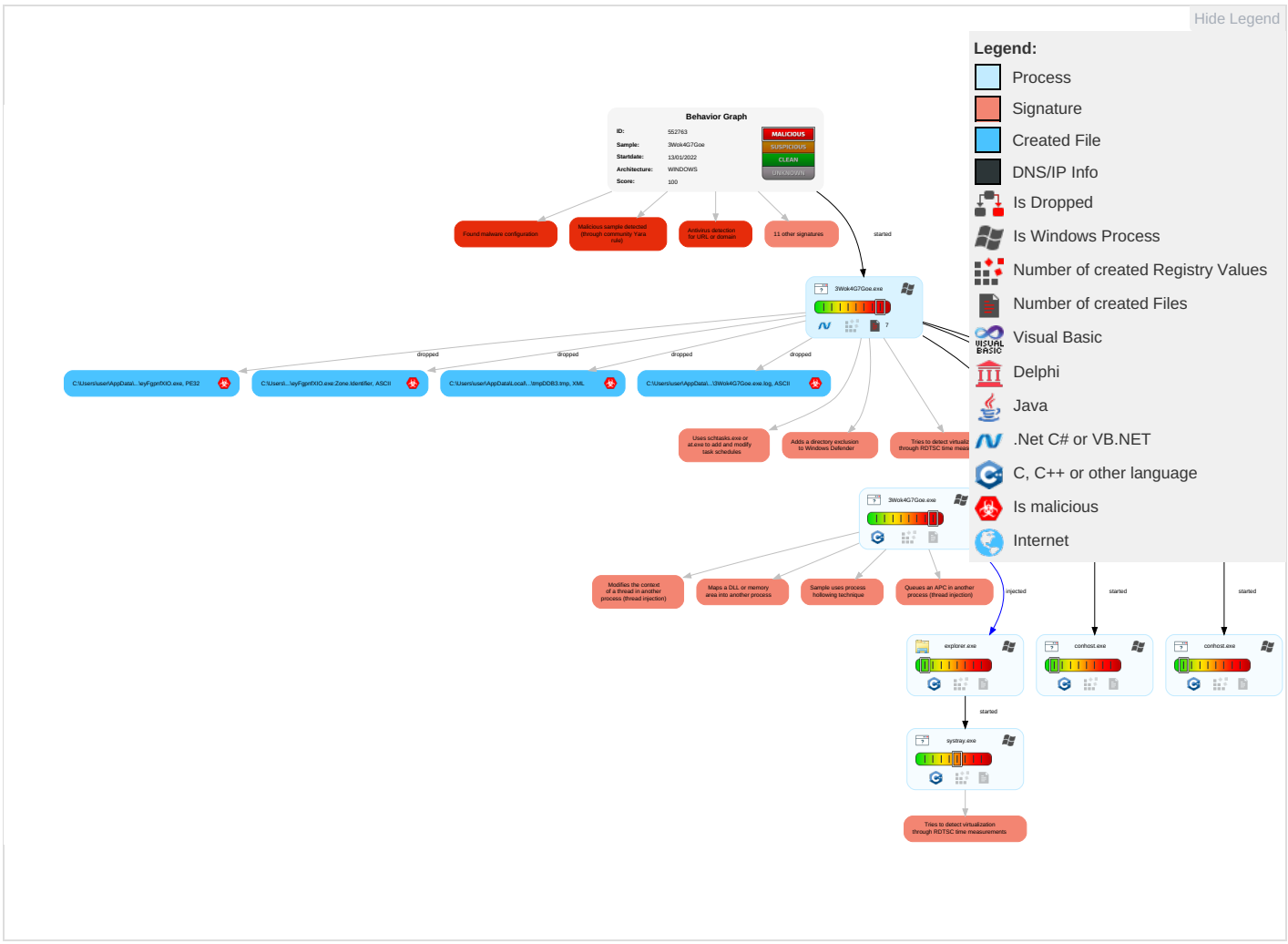
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 4 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 3 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

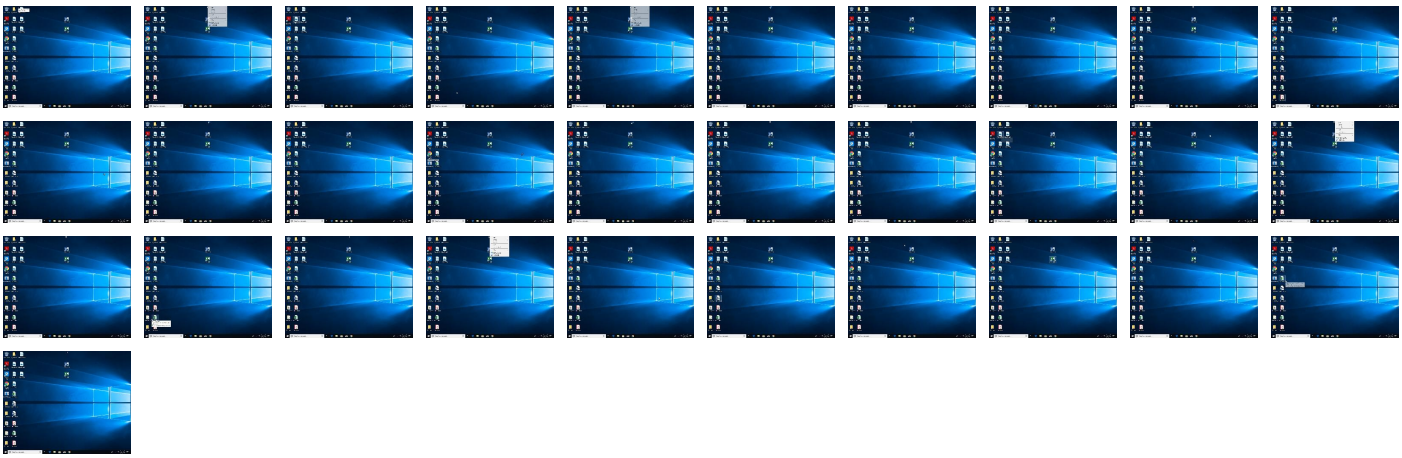
Behavior Graph



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
3Wok4G7Goe.exe	57%	Virustotal		Browse
3Wok4G7Goe.exe	71%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
3Wok4G7Goe.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe	57%	Virustotal		Browse
C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe	71%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.3Wok4G7Goe.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.0.3Wok4G7Goe.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.0.3Wok4G7Goe.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.0.3Wok4G7Goe.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
www.topeasyip.company/i5nb/	4%	Virustotal		Browse
www.topeasyip.company/i5nb/	100%	Avira URL Cloud	malware	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.topeasyip.company/i5nb/	true	• 4%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552763
Start date:	13.01.2022
Start time:	17:55:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3Wok4G7Goe (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 14.3% (good quality ratio 12.6%) • Quality average: 67.8% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:56:09	API Interceptor	1x Sleep call for process: 3Wok4G7Goe.exe modified
17:56:13	API Interceptor	25x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3Wok4G7Goe.exe.log	
Process:	C:\Users\user\Desktop\3Wok4G7Goe.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22176
Entropy (8bit):	5.60504516282984
Encrypted:	false
SSDEEP:	384:GtCDSC0yzk37W0EbT+RYSBKnQjultIir7Y9gtrSJ3xyT1MarZlbAV7BW0xk5ZBDG:9A37WN34KQCltdvhcoCafw12VG
MD5:	2AA55097F66E4094D1EF892A5C461FC0
SHA1:	A4F00FB464D6BC8AF343D7EF667E64D2A6C0E454
SHA-256:	79D4F6DA4AE6E13A5DBB5A529D74FA4A5DF81928D17C620D27352C5E10409AD3
SHA-512:	E4FBB55F85CA83AB29D52B01D8238FDCF5E96E1CFA110D3E6F1220FEE0C5BED264E76E14779C422449F94573C4DA7B1E8B7AC089FF7D9236EE1A45D4A2A85A DB
Malicious:	false
Reputation:	low
Preview:	@...e.....`.....h.....y...l.....@.....H.....<@.^.L."My...:<..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ajkuautj.dhg.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mxomvrbi.i11.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mxomvrbi.i11.psm1	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpDDB3.tmp	
Process:	C:\Users\user\Desktop\3Wok4G7Goe.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1613
Entropy (8bit):	5.131369287800644
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtG5xvn:cgeHMYrFdOFzOzN33ODOiDdKrsuTGvv
MD5:	25A2B4DAA223C0F8C9387E98A318191D
SHA1:	B060752439DC502DE7687311280BCA3599778F34
SHA-256:	573F1203824D3733583A58C82056E7F0EC23F438E7B5C79D630B0061ADCFF196
SHA-512:	E7C8BA0ECE1D751355A2DB4685785691768182D751F8B78488C4C45A646B566A4341F952FB6B74518EC8D51F76856131E585848EFD0EF77BF71A7C3F42D91A5B
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvai

C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe	
Process:	C:\Users\user\Desktop\3Wok4G7Goe.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	376832
Entropy (8bit):	7.925706696320029
Encrypted:	false
SSDEEP:	6144:JOYt1DBzXwYUnZzlCezd6O53Y5E/XL4yHnu6yvQgtLMDatOerX/D8tbkrDNrfA:JOYdLUZzlCeR6B5qL/7qtLdtF/4JkPNE
MD5:	1E14373563BCF10103F2850B17B100EA
SHA1:	F19D6F0A506F86025EE25AB6AD9405E4BC297783
SHA-256:	8D38BE02AB71FBA9115C3A645EDF515C62FFE53A5A590F7B37F362AB117473A1
SHA-512:	53D73E08D7668AD636DF53C10846C810507419F92017403EFD100A376B31AF5169E6A5F71D6F1248084472328F75B40B7502B1899F4C89CEDFA27AD3BE09795C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 57%, Browse • Antivirus: ReversingLabs, Detection: 71%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....@.. ....@.....K.....@..... ....H.....text..... ....`.rsrc...@.....@..@.rel oc.....@..B.....H.....i...h.....C...%.....*".(.....*.~....*.....*>.(.....X(.....*>.(.....Y(.....*>#.....@.....*B.(.....}....*..*r.r...p.{....o ....(....(....z"..(....*..s....*B.(.....}....*r.r...p.{....o....(....(....z.s*...*"..o+...*"..o,...*"..o-...*&...(....*..o/...*..o0...*..o1...*"..(2...*"..(3...*"..(4...*.s5...*"..o6...*"..o7...*"..o8...*..(9...*..o:...*..(;...*...}.....(A.....}.....}.....(I....*>..(.....*..oU...*..oV...

C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\3Wok4G7Goe.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64

C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe:Zone.Identifier	
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220113\PowerShell_transcript.103386.3rTMab6k.20220113175612.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	5.384597114153019
Encrypted:	false
SSDEEP:	96:BZ/6tNZqDo1ZiZ56tNZqDo1Zg28ujZA6tNZqDo1Z3DeejZY:j
MD5:	23661F1F5FCF9EAD62A79FFFC5FC82D0
SHA1:	A642BCC79C3BE8AB2B8E77384EFDAD1B4648D4F7
SHA-256:	DAE4EB2A34D9BE0E180B662F7C0757A548039DD09E4388EA2AB83ED989A91EF6
SHA-512:	BA538126667F671088CABC07B41D51D1AD18759B9B40A5CD533431CA189A865BC2EA46D31741326267DC6B920A07042C989173A62D0D8944E6F26E677FDC42DI
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220113175613..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe..Process ID: 6748..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220113175613..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe..**********..Windows PowerShell transcript start..Start time: 20220113175930..Username: computer\user..RunAs User:

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.925706696320029
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	3Wok4G7Goe.exe
File size:	376832
MD5:	1e14373563bcf10103f2850b17b100ea
SHA1:	f19d6f0a506f86025ee25ab6ad9405e4bc297783
SHA256:	8d38be02ab71fba9115c3a645edf515c62ffe53a5a590f7b37f362ab117473a1
SHA512:	53d73e08d7668ad636df53c10846c810507419f92017403efd100a376b31af5169e6a5f71d6f1248084472328f75b40b7502b1899f4c89cedfa27ad3be09795c
SSDEEP:	6144:JOYt1DBzXwYUnZzlCezd6O53Y5E/XL4yHnu6yvQgtLMDatOerX/D8tbkrDNrfA:JOYdLUZzlCeR6B5qL/7qtLdtF/4JkPNE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... ....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x45d2ee

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61DDDDDB [Tue Jan 11 19:43:23 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5b2f4	0x5b400	False	0.943608197774	data	7.93992024133	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x640	0x800	False	0.33642578125	data	3.50422251028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x60000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 3Wok4G7Goe.exe PID: 6492 Parent PID: 4504

General

Start time:	17:56:00
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\3Wok4G7Goe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\3Wok4G7Goe.exe"
Imagebase:	0xff0000
File size:	376832 bytes
MD5 hash:	1E14373563BCF10103F2850B17B100EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.284483243.000000000352B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.284413072.00000000034E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.284841170.00000000044E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.284841170.00000000044E9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.284841170.00000000044E9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6748 Parent PID: 6492

General

Start time:	17:56:10
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\eyFgpnfXIO.exe
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6756 Parent PID: 6748

General

Start time:	17:56:11
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6784 Parent PID: 6492

General

Start time:	17:56:11
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\eyFgpnfXIO" /XML "C:\Users\user\AppData\Local\Temp\tmpDDB3.tmp
Imagebase:	0x1040000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6888 Parent PID: 6784

General

Start time:	17:56:12
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 3Wok4G7Goe.exe PID: 6948 Parent PID: 6492

General

Start time:	17:56:14
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\3Wok4G7Goe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\3Wok4G7Goe.exe
Imagebase:	0xf30000
File size:	376832 bytes
MD5 hash:	1E14373563BCF10103F2850B17B100EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.281378639.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.281378639.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.281378639.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.346591920.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.346591920.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.346591920.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.347595779.0000000001490000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.347595779.0000000001490000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.347595779.0000000001490000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.280991422.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.280991422.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.280991422.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.347386368.0000000001460000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.347386368.0000000001460000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.347386368.0000000001460000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 6948

General

Start time:	17:56:21
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.329933036.0000000007FAD000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.329933036.0000000007FAD000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.329933036.0000000007FAD000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.311709571.0000000007FAD000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.311709571.0000000007FAD000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.311709571.0000000007FAD000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: systray.exe PID: 6552 Parent PID: 3292

General

Start time:	17:56:45
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0x100000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.514743460.0000000002130000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.514743460.0000000002130000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.514743460.0000000002130000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.517168088.0000000003F40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.517168088.0000000003F40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.517168088.0000000003F40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.517434675.0000000003FA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.517434675.0000000003FA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.517434675.0000000003FA0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis