JoeSandbox Cloud BASIC

ID: 552749
Sample Name:
52h0KETBXt.exe
Cookbook: default.jbs
Time: 17:41:02
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

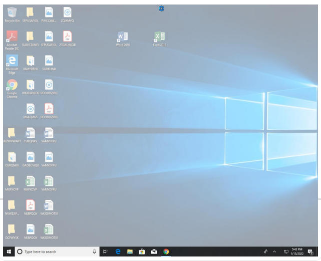
Windows Analysis Report 52h0KETBXt.exe

Overview

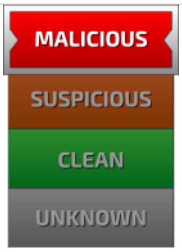
General Information

Sample Name:	52h0KETBXt.exe
Analysis ID:	552749
MD5:	c0fed64dae580ef..
SHA1:	d7de3d945c5e62..
SHA256:	5bd07db2eed6c7..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



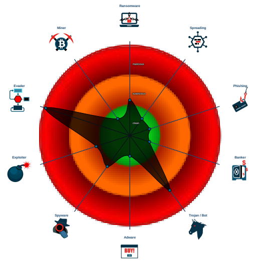
FormBook

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
- Multi AV Scanner detection for doma…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- 52h0KETBXt.exe (PID: 1360 cmdline: "C:\Users\user\Desktop\52h0KETBXt.exe" MD5: C0FED64DAE580EFB8FB8308ACCF76CAC)
  - 52h0KETBXt.exe (PID: 984 cmdline: C:\Users\user\Desktop\52h0KETBXt.exe MD5: C0FED64DAE580EFB8FB8308ACCF76CAC)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 5652 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - autoconv.exe (PID: 5656 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - systray.exe (PID: 5644 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
        - cmd.exe (PID: 5468 cmdline: /c del "C:\Users\user\Desktop\52h0KETBXt.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 5104 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hstolchsjybyl.com/a83r/"
  ],
  "decoy": [
    "comercializadoralonso.com",
    "durhamschoolservces.com",
    "onegreencapital.com",
    "smartcities24.com",
    "maquinas.store",
    "brianlovesbonsai.com",
    "xin41518s.com",
    "moneyearnus.xyz",
    "be-mix.com",
    "fengyat.club",
    "inspectdecided.xyz",
    "paksafpakistan.com",
    "orhidlnt.top",
    "princesuraj.com",
    "vietnamvodka.com",
    "renewnow.site",
    "imageservices.xyz",
    "luxurytravelfranchise.com",
    "kp112.red",
    "royalyorkfirewood.com",
    "azharrizvi.com",
    "mtvamazon.com",
    "stlouisplatinumhomes.com",
    "ke6rkmtn.xyz",
    "roomviser.xyz",
    "rollcalloutfitters.com",
    "jlautoparts.net",
    "swipyy.xyz",
    "handymansaltlakecity.com",
    "tuespr.com",
    "prelink.xyz",
    "whrpky037.xyz",
    "yoga-4-health.com",
    "silvermoonandcompany.com",
    "meg-roh.com",
    "81218121.com",
    "prayerteamusa.com",
    "ocejxu.com",
    "lopeyhomeimporvementservice.com",
    "dcosearchandconnect.xyz",
    "md-newspages.online",
    "elinmex.online",
    "traineriq.com",
    "feministecologies.com",
    "gyltogether.com",
    "polyversed.com",
    "rodolforios.com",
    "bcfs0l.com",
    "51dmm.com",
    "metaverselivecasinos.com",
    "csjsgk.com",
    "impactincentivesregistry.com",
    "firekim.space",
    "jdzn.xyz",
    "d6ybf7yj.xyz",
    "sturt.xyz",
    "serious-cam.com",
    "stihl-gms.com",
    "gentleman5.xyz",
    "rustbeltcoders.net",
    "hmarketsed96.com",
    "cricfreelive.com",
    "wellyounow.com",
    "fwdrow.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.679463516.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.679463516.0000000000400000.00000040.00000001.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1b937:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1c93a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000000.679463516.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x18859:$sqlite3step: 68 34 1C 7B E1 0x1896c:$sqlite3step: 68 34 1C 7B E1 0x18888:$sqlite3text: 68 38 2A 90 C5 0x189ad:$sqlite3text: 68 38 2A 90 C5 0x1889b:$sqlite3blob: 68 53 D8 7F 8C 0x189c3:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.929865713.0000000000470000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.929865713.0000000000470000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x9908:$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 0x1b937:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1c93a:$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
2.0.52h0KETBXt.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.52h0KETBXt.exe.400000.8.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:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1ab37:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1bb3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.52h0KETBXt.exe.400000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x17a59:$sqlite3step: 68 34 1C 7B E1 0x17b6c:$sqlite3step: 68 34 1C 7B E1 0x17a88:$sqlite3text: 68 38 2A 90 C5 0x17bad:$sqlite3text: 68 38 2A 90 C5 0x17a9b:$sqlite3blob: 68 53 D8 7F 8C 0x17bc3:$sqlite3blob: 68 53 D8 7F 8C
2.2.52h0KETBXt.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.52h0KETBXt.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x8b08:$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 83 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 0x1ab37:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1bb3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 18 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Multi AV Scanner detection for domain / URL
- Machine Learning detection for sample

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
- .NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection:

- Self deletion via cmd delete

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
- Injects a PE file into a foreign processes
- 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

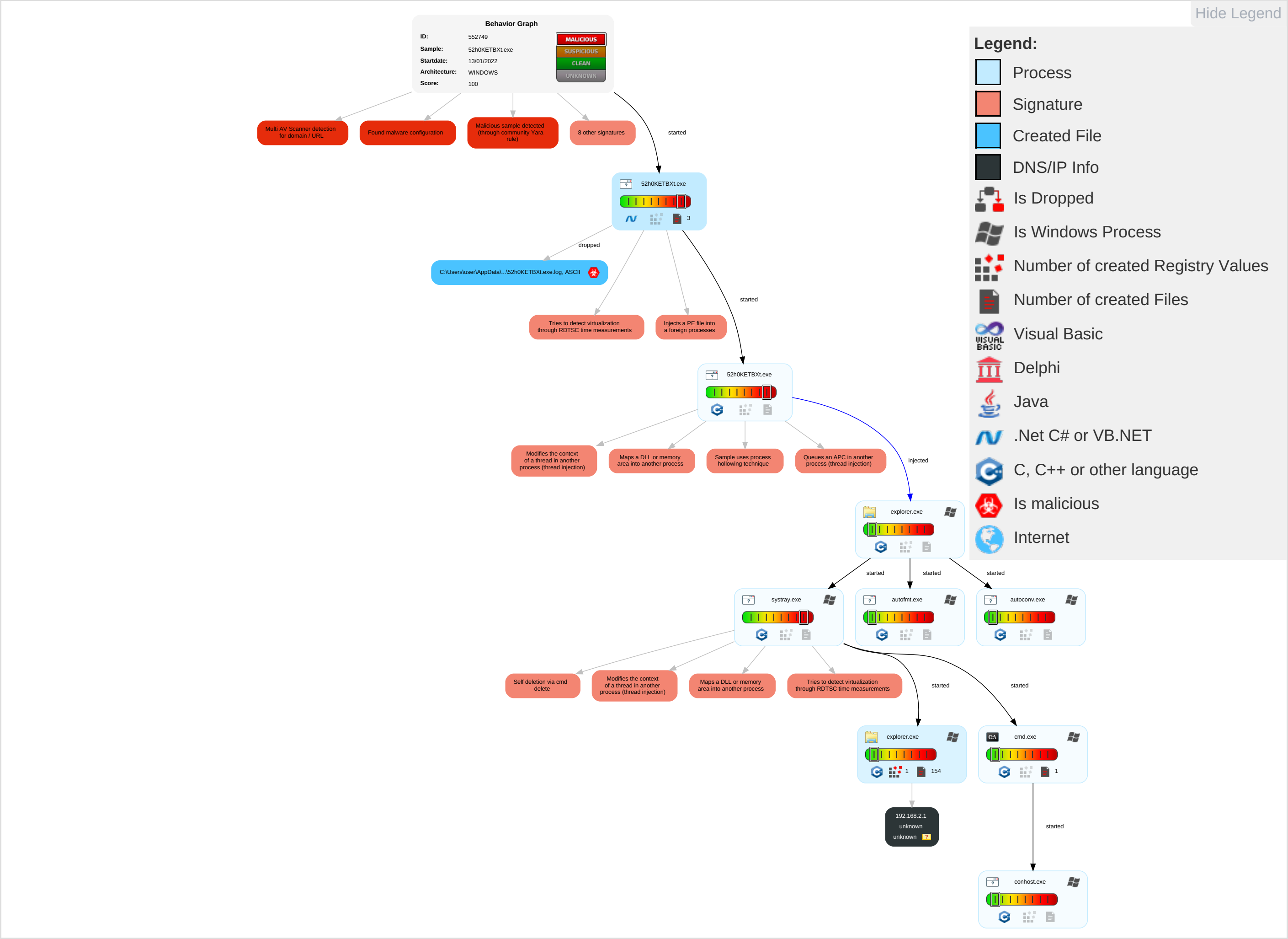
Remote Access Functionality:

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
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	Process Injection 5 1 2	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop c Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Virtualization/Sandbox Evasion 4 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 Communica
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 2 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statior

Behavior Graph



Behavior Graph

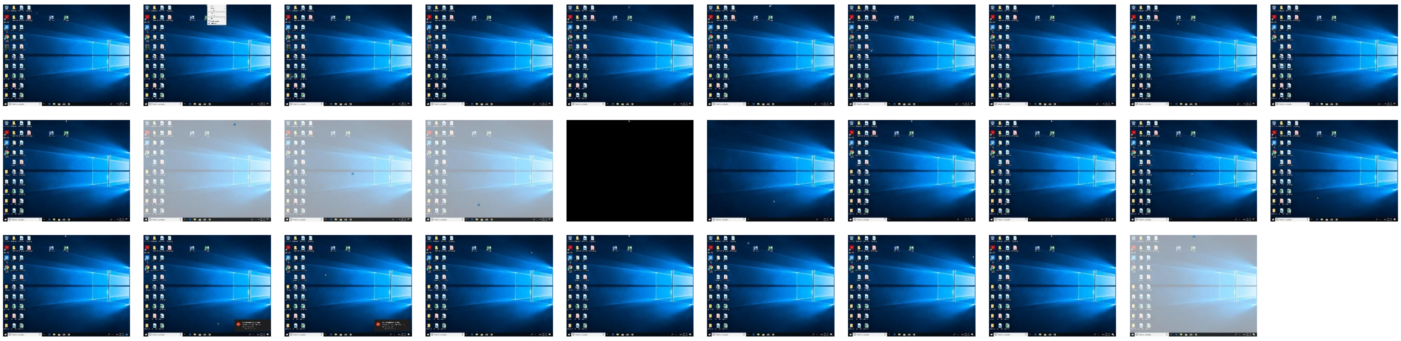
ID: 552749
Sample: 52h0KETBXt.exe
Startdate: 13/01/2022
Architecture: WINDOWS
Score: 100

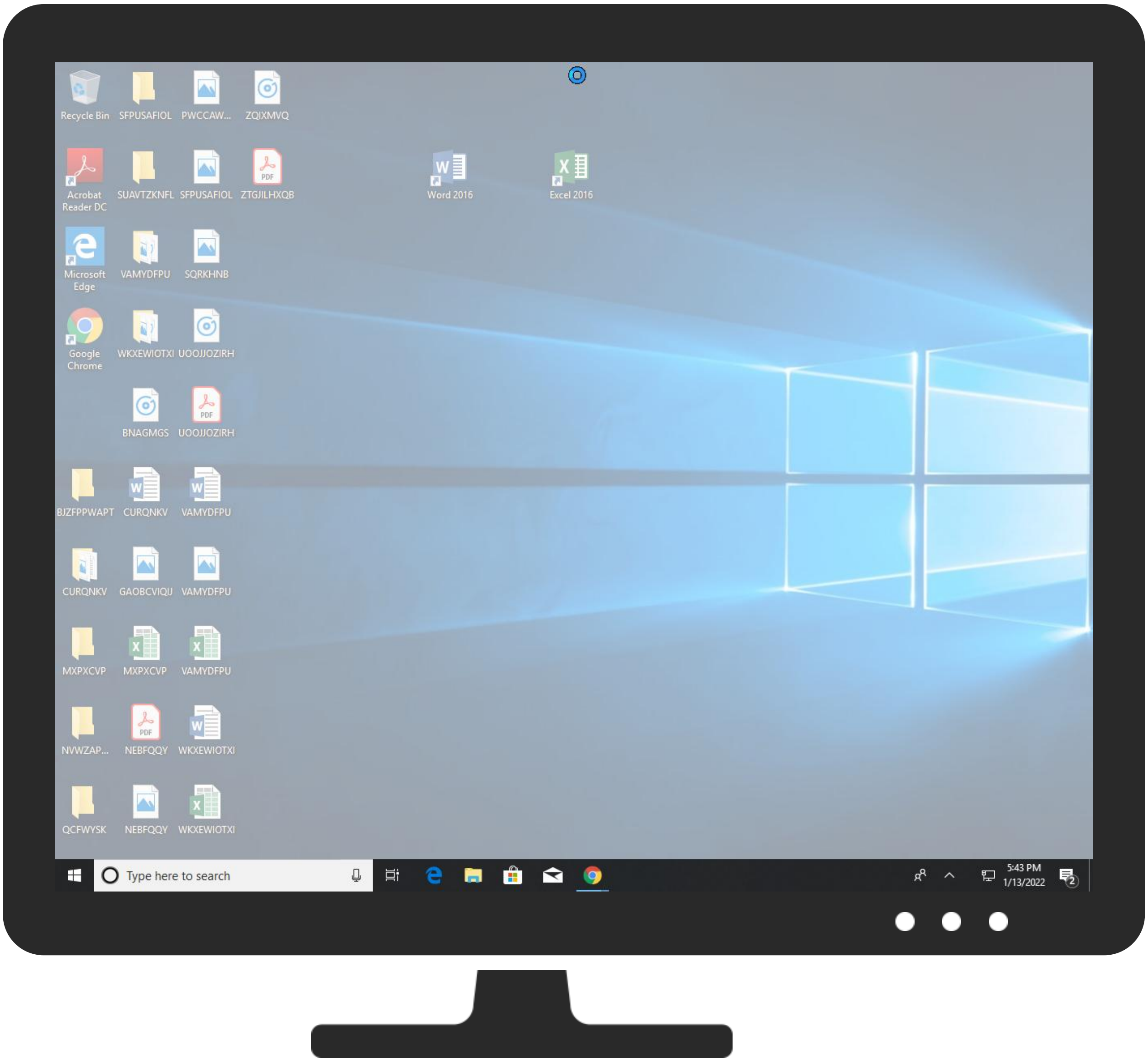
Hide Legend
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Multi AV Scanner detection for domain / URL
Found malware configuration
Malicious sample detected (through community Yara rule)
8 other signatures
started
52h0KETBXt.exe
3
dropped
C:\Users\user\AppData\...\52h0KETBXt.exe.log, ASCII
Tries to detect virtualization through RDTSC time measurements
Injects a PE file into a foreign processes
started
52h0KETBXt.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Sample uses process hollowing technique
Queues an APC in another process (thread injection)
injected
explorer.exe
started
started
started
systray.exe
autofmt.exe
autoconv.exe
Self deletion via cmd delete
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Tries to detect virtualization through RDTSC time measurements
started
started
explorer.exe
1
154
cmd.exe
C:\
1
192.168.2.1
unknown
unknown
started
conhost.exe
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

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
52h0KETBXt.exe	34%	Virustotal		Browse
52h0KETBXt.exe	39%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
52h0KETBXt.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.52h0KETBXt.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.52h0KETBXt.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.52h0KETBXt.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.52h0KETBXt.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnK	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.como.?	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.comiona	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.galapagosdesign.com/1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/;	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
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	
http://www.founder.com.cn/cni	0%	URL Reputation	safe	
www.hstolchsjybyl.com/a83r/	5%	Virustotal		Browse
www.hstolchsjybyl.com/a83r/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.hstolchsjybyl.com/a83r/	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552749
Start date:	13.01.2022
Start time:	17:41:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	52h0KETBXt.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:	27
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@10/1@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 20.9% (good quality ratio 18.9%) • Quality average: 69.6% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:42:03	API Interceptor	1x Sleep call for process: 52h0KETBXt.exe modified
17:43:07	API Interceptor	284x Sleep call for process: explorer.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\52h0KETBXt.exe.log	
Process:	C:\Users\user\Desktop\52h0KETBXt.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	**true**
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.595409513386053
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	52h0KETBXt.exe
File size:	488960
MD5:	c0fed64dae580efb8fb8308accf76cac
SHA1:	d7de3d945c5e62ee8f7b77a508b8b0682cae713d
SHA256:	5bd07db2eed6c7e67e3f3947b5336c6ba986cfbd03bd406 c13eda1999a64fc70
SHA512:	1ffb0f66a59f98cd4d289b2c7baf0a96e025aa2dced1351d 3359ee3b0491975bbe433669253fcc211a507eead2bd53 0fdf46aba421c55f1d52bd069858fc98d3
SSDEEP:	12288:KLOPQWlRGF/Z3I5tefhiKwVD2EpioIYaE252hhW:KLOIW+FWfMir2E4oLg5gI
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......a.............0..(...L......2F... ...`....@.. ....@................................

File Icon

Icon Hash:	ce9c9496e4949c9e

Static PE Info

General

Entrypoint:	0x474632
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:	0x61DF84F6 [Thu Jan 13 01:48:38 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	0x72650	0x72800	False	0.847104001774	data	7.63059503702	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x48a8	0x4a00	False	0.546611064189	data	6.20583800689	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c000	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: 52h0KETBXt.exe PID: 1360 Parent PID: 5188

General

Start time:	17:41:54
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\52h0KETBXt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\52h0KETBXt.exe"
Imagebase:	0x4d0000
File size:	488960 bytes
MD5 hash:	C0FED64DAE580EFB8FB8308ACCF76CAC
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: 00000001.00000002.682151005.00000000028F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.682235184.0000000002994000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.682477718.00000000038F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.682477718.00000000038F9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.682477718.00000000038F9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Analysis Process: 52h0KETBXt.exe PID: 984 Parent PID: 1360

General

Start time:	17:42:04
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\52h0KETBXt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\52h0KETBXt.exe
Imagebase:	0x430000
File size:	488960 bytes
MD5 hash:	C0FED64DAE580EFB8FB8308ACCF76CAC

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: 00000002.00000000.679463516.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.679463516.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.679463516.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.740647599.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.740647599.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.740647599.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.741087450.0000000000A30000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.741087450.0000000000A30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.741087450.0000000000A30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.679919351.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.679919351.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.679919351.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.741186169.0000000000E60000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.741186169.0000000000E60000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.741186169.0000000000E60000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 984

General

Start time:	17:42:07
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: 00000003.00000000.713850034.000000000DAB7000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.713850034.000000000DAB7000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.713850034.000000000DAB7000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.729857444.000000000DAB7000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.729857444.000000000DAB7000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.729857444.000000000DAB7000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: autofmt.exe PID: 5652 Parent PID: 3424

General

Start time:	17:42:30
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0x13c0000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: autoconv.exe PID: 5656 Parent PID: 3424

General

Start time:	17:42:31
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x10a0000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: systray.exe PID: 5644 Parent PID: 3424

General

Start time:	17:42:32
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\systray.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0x2f0000
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: 00000007.00000002.929865713.0000000000470000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.929865713.0000000000470000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.929865713.0000000000470000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.932677156.0000000002840000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.932677156.0000000002840000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.932677156.0000000002840000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.932951022.0000000002940000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.932951022.0000000002940000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.932951022.0000000002940000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5468 Parent PID: 5644

General

Start time:	17:42:35
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\52h0KETBXt.exe"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5672 Parent PID: 5468

General

Start time:	17:42:36
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: explorer.exe PID: 5104 Parent PID: 4128

General

Start time:	17:43:06
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal