ID: 512165
Sample Name:
7TupDHKAwm.exe
Cookbook: default.jbs
Time: 09:04:25
Date: 30/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 7TupDHKAwm.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 15
Data Directories 15
Sections 15
Resources 15
Imports 15
Version Infos 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTP Request Dependency Graph 15
HTTP Packets 15
Code Manipulations 16
User Modules 16
Hook Summary 16
Processes 16

Statistics 16
Behavior 16
System Behavior 16
Analysis Process: 7TupDHKAwm.exe PID: 6936 Parent PID: 2512 16
General 16
File Activities 17
File Created 17
File Written 17
File Read 17
Analysis Process: 7TupDHKAwm.exe PID: 6376 Parent PID: 6936 17
General 17
File Activities 18
File Read 18
Analysis Process: explorer.exe PID: 3424 Parent PID: 6376 18
General 18
File Activities 19
Analysis Process: WWAHost.exe PID: 6024 Parent PID: 3424 19
General 19
File Activities 19
File Read 19
Analysis Process: cmd.exe PID: 4128 Parent PID: 6024 20
General 20
File Activities 20
Analysis Process: conhost.exe PID: 5380 Parent PID: 4128 20
General 20
Disassembly 20
Code Analysis 20

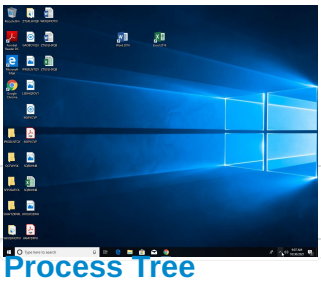
Windows Analysis Report 7TupDHKAwm.exe

Overview

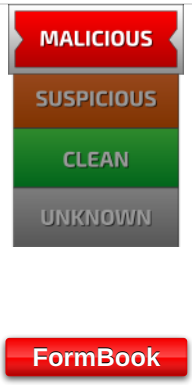
General Information

Sample Name:	7TupDHKAwm.exe
Analysis ID:	512165
MD5:	70b00a6a05ad96..
SHA1:	e51873233e7985..
SHA256:	be61aba2c5d56a..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



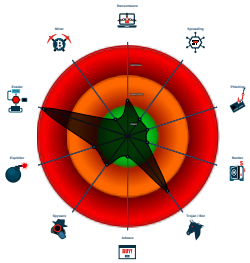
FormBook

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
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- 7TupDHKAwm.exe (PID: 6936 cmdline: 'C:\Users\user\Desktop\7TupDHKAwm.exe' MD5: 70B00A6A05AD968AF28F6B303D38F231)
  - 7TupDHKAwm.exe (PID: 6376 cmdline: C:\Users\user\Desktop\7TupDHKAwm.exe MD5: 70B00A6A05AD968AF28F6B303D38F231)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WWAHost.exe (PID: 6024 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 4128 cmdline: /c del 'C:\Users\user\Desktop\7TupDHKAwm.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.agentpathleurre.space/s18y/"
  ],
  "decoy": [
    "jokes-online.com",
    "dzzdjn.com",
    "lizzieerhardtebnaryepptts.com",
    "interfacehand.xyz",
    "sale-m.site",
    "block-facebook.com",
    "dicasdamadrinha.com",
    "maythewind.com",
    "hasari.net",
    "omnists.com",
    "thevalley-eg.com",
    "rdfj.xyz",
    "szhfcy.com",
    "alkalineage.club",
    "fdf.xyz",
    "absorplus.com",
    "poldolongo.com",
    "badassshirts.club",
    "ferienwohnungenmv.com",
    "bilboondokoak.com",
    "ambrosiaaudio.com",
    "lifeneurologyclub.com",
    "femboys.world",
    "blehmails.com",
    "gametimebg.com",
    "duytienauto.net",
    "owerful.com",
    "amedicalsupplyco.com",
    "americonnlogistics.com",
    "ateamautoglassga.com",
    "clickstool.com",
    "fzdzcnj.com",
    "txtgo.xyz",
    "izassist.com",
    "3bangzhu.com",
    "myesstyle.com",
    "aek181129aek.xyz",
    "daoxinghumaotest.com",
    "jxdg.xyz",
    "restorationculturecon.com",
    "thenaturalnutrient.com",
    "sportsandgames.info",
    "spiderwebinar.net",
    "erqgseidx.com",
    "donutmastermind.com",
    "aidatislemleri-govtr.com",
    "weetsist.com",
    "sunsetschoolportaits.com",
    "exodusguarant.tech",
    "gsnbls.top",
    "huangdashi33.xyz",
    "amazonretoure.net",
    "greathomeinlakewood.com",
    "lenovoidc.com",
    "qiuhenglawfirm.com",
    "surveyorslimited.com",
    "carterscts.com",
    "helmosy.online",
    "bakersfieldlaughingstock.com",
    "as-payjrku.icu",
    "mr-exclusive.com",
    "givepy.info",
    "ifvita.com",
    "obesocarpinteria.online"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.742059304.0000000001830000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.742059304.0000000001830000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.742059304.0000000001830000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$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:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.922711515.0000000000A10000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.922711515.0000000000A10000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.7TupDHKAwm.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.7TupDHKAwm.exe.400000.4.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.0.7TupDHKAwm.exe.400000.4.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
6.2.7TupDHKAwm.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.7TupDHKAwm.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$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 • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 20 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

Networking:

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

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

Hooking and other Techniques for Hiding and Protection:

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

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:

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

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

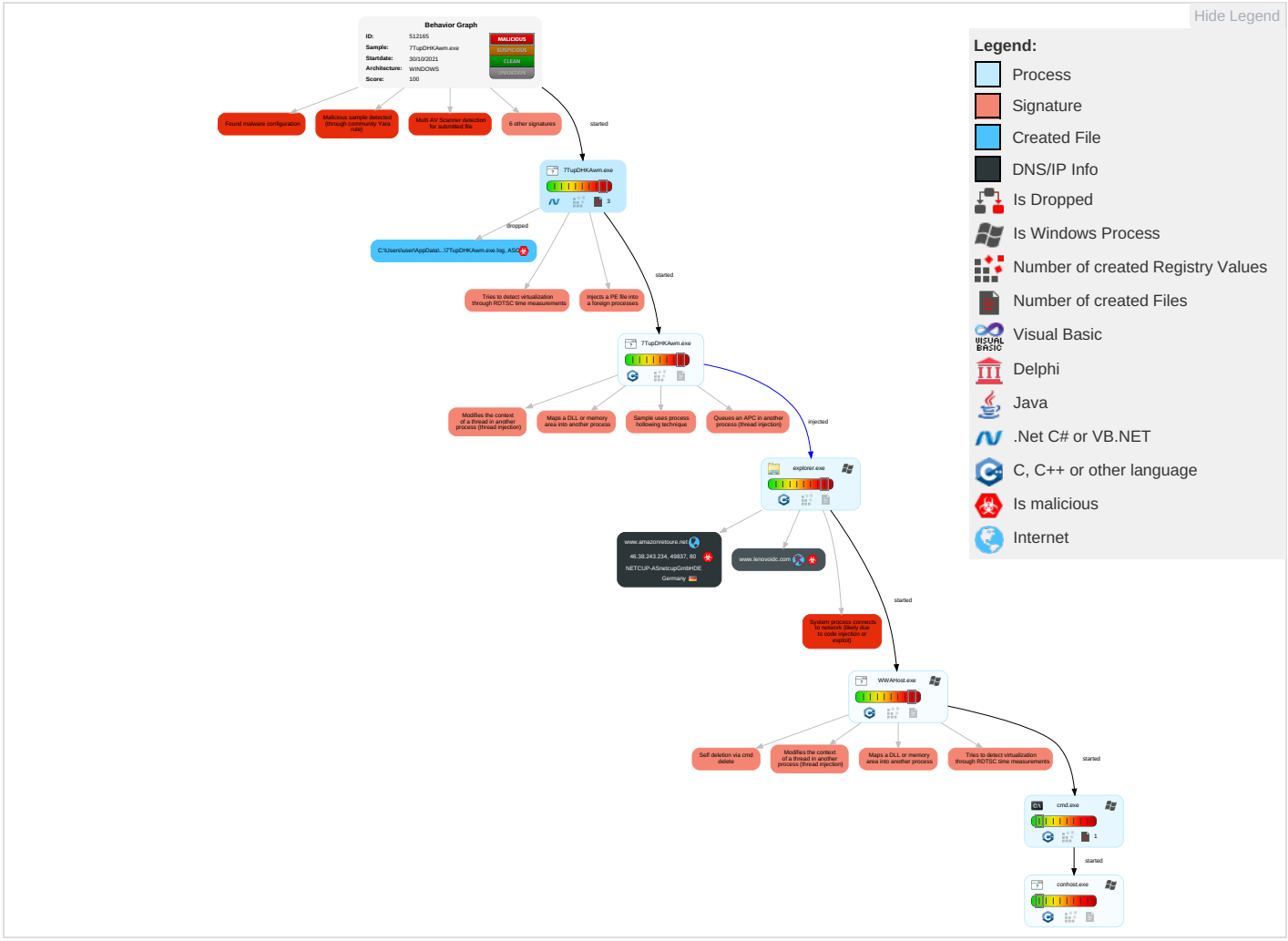
Remote Access Functionality:

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	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	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 Statio

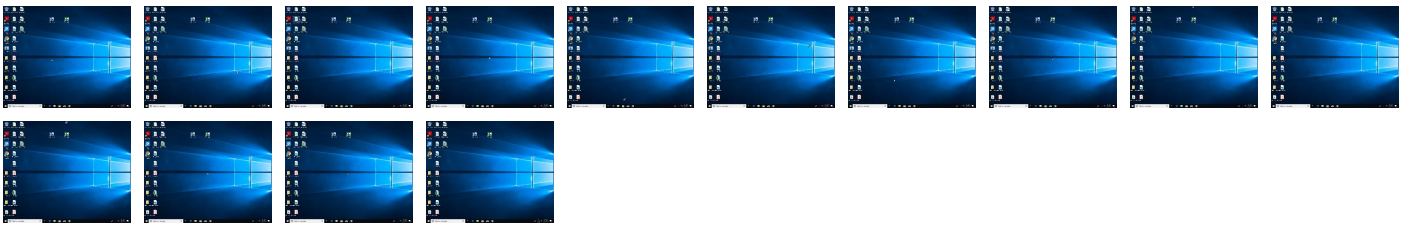
Behavior Graph



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
7TupDHKAwm.exe	19%	Virustotal		Browse
7TupDHKAwm.exe	14%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.7TupDHKAwm.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.7TupDHKAwm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.7TupDHKAwm.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.7TupDHKAwm.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/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comicet	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	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.fontbureau.comgrita	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	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.amazonretoure.net/s18y/?oVJ4Hplp=C+VjjyIyz5JhIAiSdyGuho+nJXOtpZEvhjPesU35WHH5HFWifcx9eas6lvx4xbPC6vhC&TlZlo=3fdTDXLHN2n	0%	Avira URL Cloud	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	
www.agentpathleurre.space/s18y/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.amazonretoure.net	46.38.243.234	true	true		unknown
www.lenovoidc.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.amazonretoure.net/s18y/?oVJ4Hplp=C+VjjyIyz5JhIAiSdyGuho+nJXOtpZEvhjPesU35WHH5HFWifcx9eas6lvx4xbPC6vhC&TlZlo=3fdTDXLHN2n	true	• Avira URL Cloud: safe	unknown
www.agentpathleurre.space/s18y/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.38.243.234	www.amazonretoure.net	Germany		197540	NETCUP-ASnetcupGmbHDE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	512165
Start date:	30.10.2021
Start time:	09:04:25

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7TupDHKAwm.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:	21
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@7/1@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.1% (good quality ratio 20%) • Quality average: 71.4% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 99% • 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
09:05:28	API Interceptor	1x Sleep call for process: 7TupDHKAwm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
46.38.243.234	9LjOeq9jnl.exe	Get hash	malicious	Browse	• www.qumpan.com/shjn/?UTqtRv=yig434buSM9mjL6sFft/wR3J8yL+W/NNnR041iD/jBfLeA0894Dqi/iq5ABbTrmmBq9f&Whc=0DHdArEp5hQd

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OApfyh3Vfm.exe	Get hash	malicious	Browse	• www.qumpan.com/shjn/?BZXds2=yig434buSM9mjL6sFft/wR3J8yL+W/NNnR041iD/jBfLeA0894Dqi/iq5ABxMbWmFo1f&jlW=5jlhet3

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NETCUP-ASnetcupGmbHDE	9LjOeq9jnl.exe	Get hash	malicious	Browse	• 46.38.243.234
	OApfyh3Vfm.exe	Get hash	malicious	Browse	• 46.38.243.234
	ozJy5Zf5cf.exe	Get hash	malicious	Browse	• 46.38.235.14
	soezuiIhz2	Get hash	malicious	Browse	• 193.31.25.205
	JNk46WKTxo.exe	Get hash	malicious	Browse	• 92.60.36.153
	y2N49ht6t4.exe	Get hash	malicious	Browse	• 194.55.13.50
	zfpLjnr5P9.exe	Get hash	malicious	Browse	• 5.45.111.149
	re2.arm	Get hash	malicious	Browse	• 37.120.179.69
	Z9GkJvygEk.exe	Get hash	malicious	Browse	• 188.68.46.164
	5PfBAmWq3V.exe	Get hash	malicious	Browse	• 188.68.46.164
	BCf7GIQnLJ.exe	Get hash	malicious	Browse	• 152.89.104.58
	WlWQ2rh08n.exe	Get hash	malicious	Browse	• 37.120.190.6
	oPi2xY65IJ.exe	Get hash	malicious	Browse	• 194.55.13.50
	2te6IkdbJu.exe	Get hash	malicious	Browse	• 185.244.192.247
	UBHfmKPqlV.exe	Get hash	malicious	Browse	• 185.163.117.111
	75dZK4LPMP.exe	Get hash	malicious	Browse	• 45.136.31.178
	VCJQWUG1iY.exe	Get hash	malicious	Browse	• 37.120.174.249
	v6TB5C7KtW.exe	Get hash	malicious	Browse	• 37.120.169.172
	SecuriteInfo.com.W32.MSIL_Kryptik.EWM.genEldorado.30775.exe	Get hash	malicious	Browse	• 94.16.114.105
	7f8BlPBZMS	Get hash	malicious	Browse	• 185.170.115.35

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7TupDHKAwm.exe.log

Process:	C:\Users\user\Desktop\7TupDHKAwm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7TupDHKAwm.exe.log	
Malicious:	**true**
Reputation:	high, 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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.409457976178682
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	7TupDHKAwm.exe
File size:	422912
MD5:	70b00a6a05ad968af28f6b303d38f231
SHA1:	e51873233e79851d7ee46d1f5553cf2b4d60098d
SHA256:	be61aba2c5d56a20b50c5f4a682087840876fdf7504fbf5eb8ac56a0e572fb33
SHA512:	d81b86c15212f716c87f79fa9dc1214ac09d5f93eb109e014b13cd4adcf33413747df4b2356d7de7add21e35c4c1def163ac39edd368a2581e54a1ade87f2800
SSDEEP:	6144:J+zIQC1jkU55e+Bpy31k2vhwHCovelKywHq29BiXbcpyb7Q:UkQaYG5e8yK2ZJovegywHqCKx3Q
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....|a.....0..j..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4688f6
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:	0x617CA1D9 [Sat Oct 30 01:37:29 2021 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

General

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	0x668fc	0x66a00	False	0.819791508069	data	7.4234449666	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6a000	0x5ec	0x600	False	0.4375	data	4.23054866381	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6c000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 30, 2021 09:06:52.294708014 CEST	192.168.2.4	8.8.8.8	0xf09b	Standard query (0)	www.lenovoidc.com	A (IP address)	IN (0x0001)
Oct 30, 2021 09:07:10.891835928 CEST	192.168.2.4	8.8.8.8	0x3e19	Standard query (0)	www.amazonretoure.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 30, 2021 09:06:52.678833961 CEST	8.8.8.8	192.168.2.4	0xf09b	Name error (3)	www.lenovoidc.com	none	none	A (IP address)	IN (0x0001)
Oct 30, 2021 09:07:10.917145014 CEST	8.8.8.8	192.168.2.4	0x3e19	No error (0)	www.amazonretoure.net		46.38.243.234	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.amazonretoure.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49837	46.38.243.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 30, 2021 09:07:10.947280884 CEST	6720	OUT	GET /s18y/?oVJ4Hplp=C+Vjjylyz5JhlAiSdyGuho+nJXOtpZEvhjPesU35WHH5HFWifcx9eas6lvx4xbPC6vhC&TlZlo=3fdTDXLHN2n HTTP/1.1 Host: www.amazonretoure.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 30, 2021 09:07:10.971992016 CEST	6720	IN	HTTP/1.1 404 Not Found Date: Sat, 30 Oct 2021 07:05:50 GMT Server: Apache/2.4.10 (Debian) Content-Length: 283 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 61 6d 61 7a 6f 6e 72 65 74 6f 75 72 65 2e 6e 65 74 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.10 (Debian) Server at www.amazonretoure.net Port 80</address></body></html>

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

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 7TupDHKAwm.exe PID: 6936 Parent PID: 2512

General

Start time:	09:05:18
Start date:	30/10/2021
Path:	C:\Users\user\Desktop\7TupDHKAwm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7TupDHKAwm.exe'
Imagebase:	0xf0000
File size:	422912 bytes

MD5 hash:	70B00A6A05AD968AF28F6B303D38F231
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.686015292.0000000003409000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.686015292.0000000003409000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.686015292.0000000003409000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.685820710.0000000002401000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 7TupDHKAwm.exe PID: 6376 Parent PID: 6936

General

Start time:	09:05:29
Start date:	30/10/2021
Path:	C:\Users\user\Desktop\7TupDHKAwm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\7TupDHKAwm.exe
Imagebase:	0xe50000
File size:	422912 bytes
MD5 hash:	70B00A6A05AD968AF28F6B303D38F231
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: 00000006.00000002.742059304.0000000001830000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.742059304.0000000001830000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.742059304.0000000001830000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.741623737.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.741623737.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.741623737.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.683641477.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.683641477.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.683641477.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.742802941.0000000001BA0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.742802941.0000000001BA0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.742802941.0000000001BA0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.682941306.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.682941306.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.682941306.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6376

General

Start time:	09:05:32
Start date:	30/10/2021
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: 00000008.00000000.728776884.000000000E4BB000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.728776884.000000000E4BB000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.728776884.000000000E4BB000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.713098420.000000000E4BB000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.713098420.000000000E4BB000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.713098420.000000000E4BB000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: WWAHost.exe PID: 6024 Parent PID: 3424

General

Start time:	09:05:54
Start date:	30/10/2021
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0xbb0000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
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.00000002.922711515.0000000000A10000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.922711515.0000000000A10000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.922711515.0000000000A10000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.924521754.0000000002DA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.924521754.0000000002DA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.924521754.0000000002DA0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.922851671.0000000000B70000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.922851671.0000000000B70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.922851671.0000000000B70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4128 Parent PID: 6024

General

Start time:	09:06:00
Start date:	30/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\7TupDHKAwm.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: 5380 Parent PID: 4128

General

Start time:	09:06:01
Start date:	30/10/2021
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

Disassembly

Code Analysis