ID: 528615
Sample Name:
HkE0tD0g4NXKJfy.exe
Cookbook: default.jbs
Time: 15:07:14
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

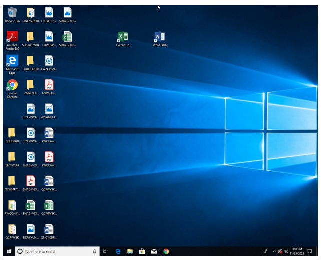
Windows Analysis Report HkE0tD0g4NXKJfy.exe

Overview

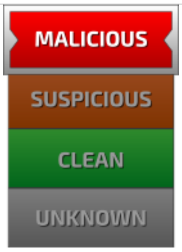
General Information

Sample Name:	HkE0tD0g4NXKJfy.exe
Analysis ID:	528615
MD5:	fcc2d1cda8d3989..
SHA1:	075de723df172cc..
SHA256:	77e1c24ecfa1d33..
Tags:	exe Formbook xloader
Infos:	

Most interesting Screenshot:



Detection



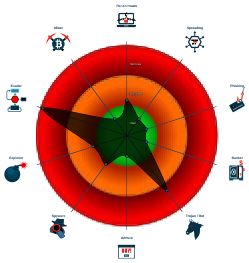
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e....
- 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…
- Self deletion via cmd delete
- .NET source code contains potentia…
- Queues an APC in another process …
- Tries to detect virtualization through…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- HkE0tD0g4NXKJfy.exe (PID: 5624 cmdline: "C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe" MD5: FCC2D1CDA8D3989FECA9C5F5F900E164)
  - HkE0tD0g4NXKJfy.exe (PID: 3336 cmdline: C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe MD5: FCC2D1CDA8D3989FECA9C5F5F900E164)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 5960 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 5904 cmdline: /c del "C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.platinumcredit.net/sh5d/"
  ],
  "decoy": [
    "officejava.store",
    "appletitan.info",
    "securebankofamericalog.site",
    "weprepareamerica-world.com",
    "suepersoldiers.com",
    "aproveiteagoras2.com",
    "harusan.website",
    "zqmm.net",
    "joinundergrad.com",
    "thefullfledged.com",
    "jadonzia.com",
    "maoshuochen.com",
    "tuntun-newmarket.com",
    "danijela-djordjevic.com",
    "usaonlinedocs.com",
    "penspanter.quest",
    "theclubhouse.tech",
    "jakital.com",
    "nj013.com",
    "foodpanda.digital",
    "arsels.info",
    "junkingcarslosangelescounty.com",
    "formaldressesforwomen.com",
    "xingruinet.ltd",
    "xcgtsret.com",
    "151motors.com",
    "realsteelsoftwaresending.com",
    "cutos2.com",
    "justifygomqbe.xyz",
    "ini91.com",
    "uniformfacilities.com",
    "bullochlifetimelegacy.com",
    "ddivfc.com",
    "tuvinoencamino.com",
    "nbtianzhou.com",
    "segmauth.com",
    "thelittlebookof52.com",
    "bellezamarket.store",
    "terrysboutique.store",
    "lightinghj.com",
    "malayray.com",
    "7routines.com",
    "costsma.net",
    "tapissier-uzes.com",
    "reparacion-termos-madrid.com",
    "combingtheratsnest.com",
    "bobcathntshop.com",
    "launchpalop.com",
    "gopheratms.com",
    "mydatingshop.com",
    "mosucoffee.club",
    "ebonyslivestockservice.online",
    "vupeliquid.com",
    "buzzsaw.club",
    "kg-zenith.com",
    "quimicosypapelesdelnte.com",
    "secure-mivote.com",
    "curatorsofkool.com",
    "quickipcheck.com",
    "ruggrunnerz.com",
    "magoro.com",
    "electricatrick.com",
    "coralload.com",
    "herhimalaya.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.346581658.0000000001450000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.346581658.0000000001450000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.346581658.0000000001450000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x16ad9:$sqlite3step: 68 34 1C 7B E1 0x16bec:$sqlite3step: 68 34 1C 7B E1 0x16b08:$sqlite3text: 68 38 2A 90 C5 0x16c2d:$sqlite3text: 68 38 2A 90 C5 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000000.323615980.000000000F7EA000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000000.323615980.000000000F7EA000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x46b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x41a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x47b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x9ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 0xac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.HkE0tD0g4NXKJfy.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.HkE0tD0g4NXKJfy.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.HkE0tD0g4NXKJfy.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x16ad9:$sqlite3step: 68 34 1C 7B E1 0x16bec:$sqlite3step: 68 34 1C 7B E1 0x16b08:$sqlite3text: 68 38 2A 90 C5 0x16c2d:$sqlite3text: 68 38 2A 90 C5 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
7.0.HkE0tD0g4NXKJfy.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.0.HkE0tD0g4NXKJfy.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

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:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:

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

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

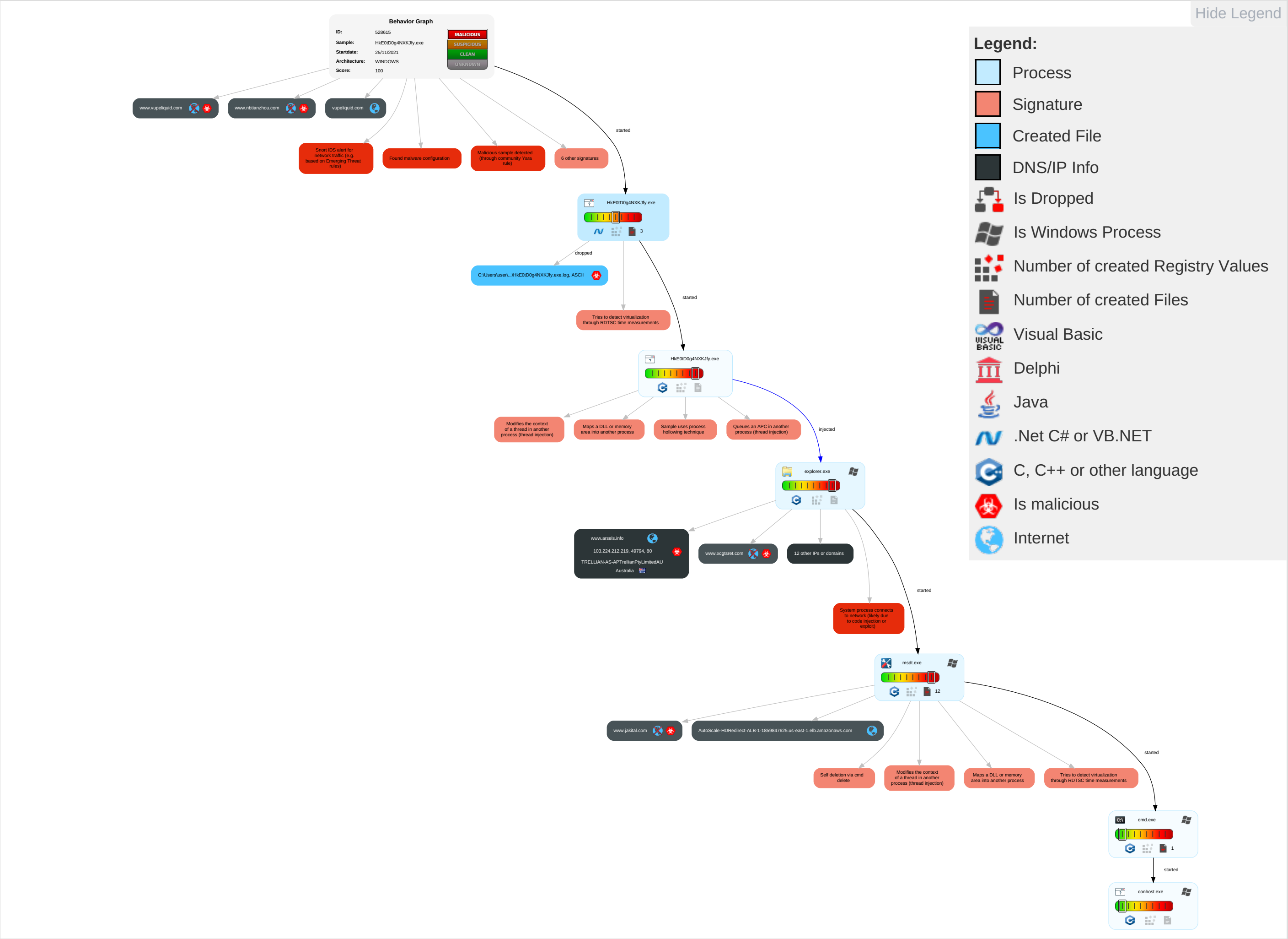
Remote Access Functionality:

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	Command and Scripting Interpreter 2	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Application Window 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	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
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 c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi- Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

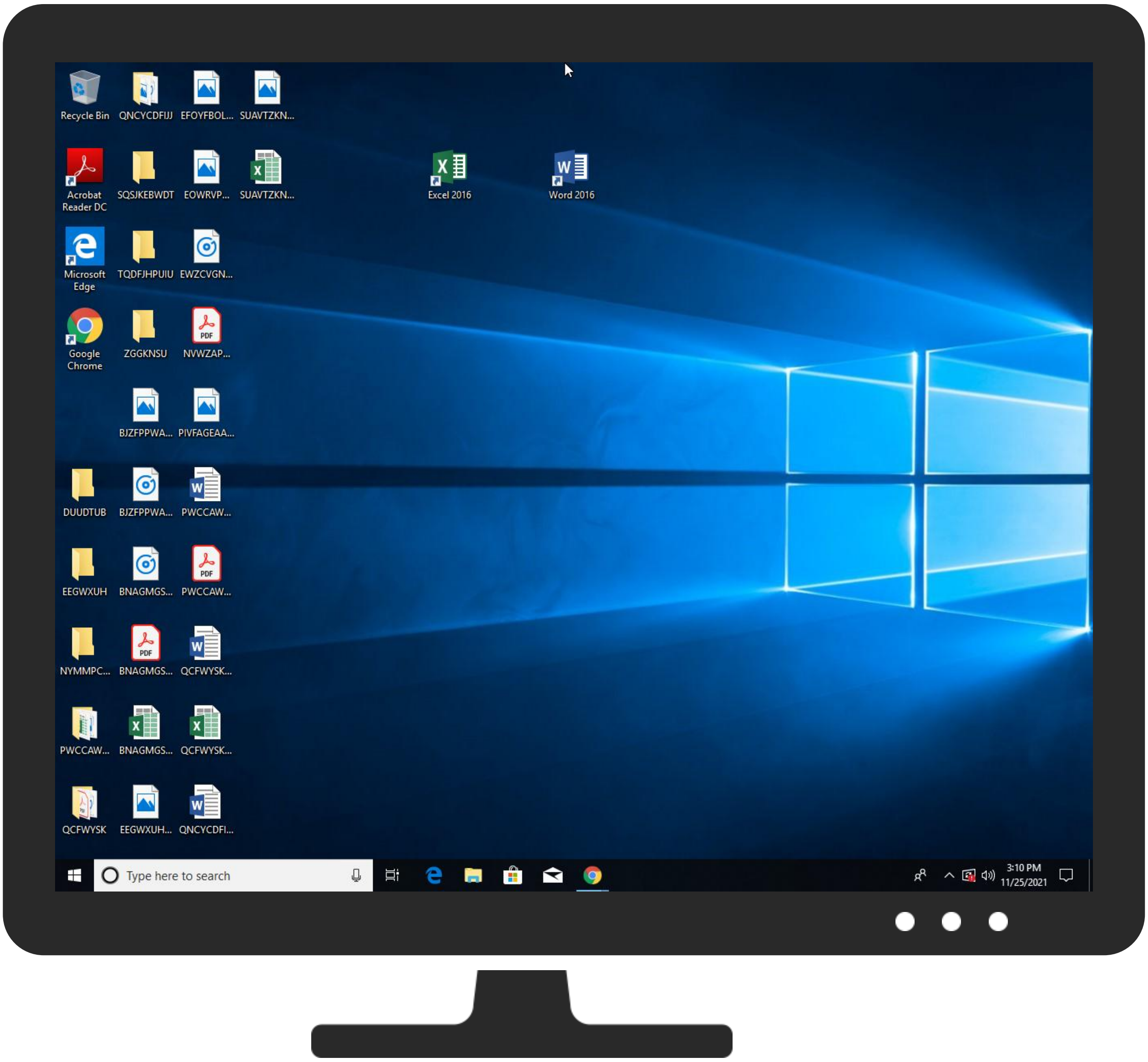
Behavior Graph


Hide Legend
Behavior Graph
ID: 528615
Sample: HkE0tD0g4NXKJfy.exe
Startdate: 25/11/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
www.vupeliquid.com
www.nbtianzhou.com
vupeliquid.com
Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Found malware configuration
Malicious sample detected (through community Yara rule)
6 other signatures
started
HkE0tD0g4NXKJfy.exe
3
dropped
C:\Users\user\...\HkE0tD0g4NXKJfy.exe.log, ASCII
Tries to detect virtualization through RDTSC time measurements
started
HkE0tD0g4NXKJfy.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
www.arsels.info
103.224.212.219, 49794, 80
TRELLIAN-AS-APTrellianPtyLimitedAU
Australia
www.xcgtsret.com
12 other IPs or domains
System process connects to network (likely due to code injection or exploit)
started
msdt.exe
12
www.jakital.com
AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com
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
cmd.exe
1
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
HkE0tD0g4NXKJfy.exe	27%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.HkE0tD0g4NXKJfy.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.0.HkE0tD0g4NXKJfy.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.0.HkE0tD0g4NXKJfy.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.HkE0tD0g4NXKJfy.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jakital.com/	0%	Avira URL Cloud	safe	
http://www.jakital.com/sh5d/?Yv=deNwNK4CD/WMHHT4cYNp3s43CKigm652n7BnZRGAFJqHojdiJSlOhFJhA2qOeK3G	0%	Avira URL Cloud	safe	
http://www.151motors.com/sh5d/?Yv=KHnqZ0TbjHhhriSsr4IC2tQHFpsEpNX6XKtcehIZDPMVzpPTFiaMMZSG67rbMC0Gdpxx&8pZ=MFQX	0%	Avira URL Cloud	safe	
http://www.suepersoldiers.com/sh5d/?Yv=SDhgbwSt5mB4DODrBIecU0Cn9nI1MHSsH0Hazkrlv9wpSquk3LdmspAinMLs2LJY3gHa&8pZ=MFQX	0%	Avira URL Cloud	safe	
www.platinumcredit.net/sh5d/	0%	Avira URL Cloud	safe	
http://www.vupeliquid.com/sh5d/?Yv=Pdn0Hokg7Q3B7dDVtUX5QMohVVbqJZ0HrhWfxUy6sRCS+GjM4sZ5xKohcZ81Ep8iPYLe&8pZ=MFQX	0%	Avira URL Cloud	safe	
http://www.arsels.info/sh5d/?Yv=U9Dn+H6I1oLCGiFi1oW/bg7Rnic0zjRPtt9AMGb5MRiLdOF7LfbhYF1T4mwo8MTrEy0Q&8pZ=MFQX	0%	Avira URL Cloud	safe	
http://www.platinumcredit.net/sh5d/?Yv=hy4EQ9RQ8H0Qmf+V5oZYawTzVdNi6YgEsN2g+zlr8kWBt8RwCZI+yMGy7WuYiu2G3qgy&8pZ=MFQX	0%	Avira URL Cloud	safe	
http://www.electricatrick.com/sh5d/?Yv=bH0MuGY0n47F1S4kOvzCBL0/mw6YL+7138CmEb6WqYz18csJYDgpNmReh/JvI3nBbY8S&8pZ=MFQX	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com	52.204.216.132	true	false		high
www.arsels.info	103.224.212.219	true	true		unknown
platinumcredit.net	34.102.136.180	true	false		unknown
electricatrick.com	34.102.136.180	true	false		unknown
151motors.com	34.102.136.180	true	false		unknown
vupeliquid.com	34.102.136.180	true	false		unknown
ghs.googlehosted.com	142.250.203.115	true	false		unknown
www.platinumcredit.net	unknown	unknown	true		unknown
www.thefullfledged.com	unknown	unknown	true		unknown
www.jakital.com	unknown	unknown	true		unknown
www.nbtianzhou.com	unknown	unknown	true		unknown
www.xcgtsret.com	unknown	unknown	true		unknown
www.151motors.com	unknown	unknown	true		unknown
www.suepersoldiers.com	unknown	unknown	true		unknown
www.vupeliquid.com	unknown	unknown	true		unknown
www.electricatrick.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.151motors.com/sh5d/?Yv=KHnqZ0TbjHhhriSsr4IC2tQHFpsEpNX6XKtcehIZDPMVzpPTFiaMMZSG67rbMC0Gdpxx&8pZ=MFQX	false	• Avira URL Cloud: safe	unknown
http://www.suepersoldiers.com/sh5d/?Yv=SDhgbwSt5mB4DODrBIecU0Cn9nI1MHSsH0Hazkrlv9wpSquk3LdmspAinMLs2LJY3gHa&8pZ=MFQX	false	• Avira URL Cloud: safe	unknown
www.platinumcredit.net/sh5d/	true	• Avira URL Cloud: safe	low
http://www.vupeliquid.com/sh5d/?Yv=Pdn0Hokg7Q3B7dDVtUX5QMohVVbqJZ0HrhWfxUy6sRCS+GjM4sZ5xKohcZ81Ep8iPYLe&8pZ=MFQX	false	• Avira URL Cloud: safe	unknown
http://www.arsels.info/sh5d/?Yv=U9Dn+H6I1oLCGiFi1oW/bg7Rnic0zjRPtt9AMGb5MRiLdOF7LfbhYF1T4mwo8MTrEy0Q&8pZ=MFQX	true	• Avira URL Cloud: safe	unknown
http://www.platinumcredit.net/sh5d/?Yv=hy4EQ9RQ8H0Qmf+V5oZYawTzVdNi6YgEsN2g+zlr8kWBt8RwCZI+yMGy7WuYiu2G3qgy&8pZ=MFQX	false	• Avira URL Cloud: safe	unknown
http://www.electricatrick.com/sh5d/?Yv=bH0MuGY0n47F1S4kOvzCBL0/mw6YL+7138CmEb6WqYz18csJYDgpNmReh/JvI3nBbY8S&8pZ=MFQX	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.115	ghs.googlehosted.com	United States	🇺🇸	15169	GOOGLEUS	false
34.102.136.180	platinumcredit.net	United States	🇺🇸	15169	GOOGLEUS	false
103.224.212.219	www.arsels.info	Australia	🇦🇺	133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true
52.204.216.132	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com	United States	🇺🇸	14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528615
Start date:	25.11.2021
Start time:	15:07:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HkE0tD0g4NXKJfy.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@13/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.5% (good quality ratio 11.8%) • Quality average: 71.7% • Quality standard deviation: 32.9%
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

Time	Type	Description
15:08:09	API Interceptor	20x Sleep call for process: HkE0tD0g4NXKJfy.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.224.212.219	11#U6708 16#U65e5 BL #U505a#U6cd5 SO NO J624 - #U9577#U5f91ISF DETAILS SO J624.exe	Get hash	malicious	Browse	• www.packyssportsbarandgrill.com/mc6b/?jHED=q6vdABYGr50+mpTbDuVjH2bXmj77a7qtsiv5Ksob526EgQZJ7eJZqZTBsliO0pE1Rz7dNSx2ew==&oDK8=OXptnZkP0zeTKbFp
	Company Profile.exe	Get hash	malicious	Browse	• www.alkalineup.info/dc02/?1bNDudv=+kLz+DEprIzY8U30IAWnamgEQgEGLSVbXudac2AKsepjAUwhwqfiCYTJlV+SA+9+XVAU&6lu=KlTl
	HIRE SOA NOV.exe	Get hash	malicious	Browse	• www.hugolabin.com/i44q/?7n=YS1dnbOkNaCP7JrmT7p6ZNFgGouLE1kKb8gf8ths3Yir/LKnwdmfPmrhsMehp4wjvOL3&b8DdKN=_b9DpJ
	RFQ - 1100195199 - 1100190814.exe	Get hash	malicious	Browse	• www.tattooof.info/nc26/?f48=ChB31lYopjmOZG3U73N52YTWorj0brdWeOA+REOz+6bldw4+nA/cQmaLai4MjdILtj65&4h50R=ABuLcpwXXr-
	November 2021 Update RFQ 3271737.exe	Get hash	malicious	Browse	• www.tattooof.info/nc26/?SBZL=ChB31lYopjmOZG3U73N52YTWorj0brdWeOA+REOz+6bldw4+nA/cQmaLai4m8t4Lphy5&D48=c2MHtVyHNxCxXp7
	32vCkFTS0X.exe	Get hash	malicious	Browse	• www.movieschor.info/qw2c/?gpt=rM2eMDGM2hRuqtSkQ+YMFWc5A7WJMLl7iFLKjR4Nu2Ciw4jbXpEUgw2kiN/aWqHDCAOD&g2=8pLpO

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U570b#U5de8--#U6cf0#U91d1#U5bf6-EXW - ETC NOV. 5 - SO C360.exe	Get hash	malicious	Browse	- www.packyssportsbarandgrill.com/mc6b/?Fb20Btg=q6vdABYGr50+mpTbDuVjH2bXmj77a7qtsiv5Ksob526EgQZJ7eJZqZTBsmOeoYYOWGSM&R0D49=XvrtZ8lP082
	RFQ - 1100195199 - 1100190914.exe	Get hash	malicious	Browse	- www.tattoof.info/nc26/?k8GXjJk=ChB31lYopjmOZG3U73N52YTWorj0brdWeOA+REOz+6bldw4+nA/cQmaLai4MjdILtj65&9rhhPx=IL3h7ZC8a4ITG4S
	RFQ - 1100195199 - 1100190914.exe	Get hash	malicious	Browse	- www.tattoof.info/nc26/?I2J=ChB31lYopjmOZG3U73N52YTWorj0brdWeOA+REOz+6bldw4+nA/cQmaLai4m8t4Lphy5&4hL0lT=KZIPBrwH1Nx4PpRp
	RFQ_PI02102110.exe	Get hash	malicious	Browse	- www.decorationnews.com/rgv6/?p8eT=YMNzjXdfi635m3k1Gzxopc8L+wUwVg6cKWqi49UbKzMkwhAgUmt+0uJBtX6FQoP4iZ3i&C0=p4sD
	PO03214890.exe	Get hash	malicious	Browse	- www.decorationnews.com/rgv6/?I6bdp0F=YMNzjXdfi635m3k1Gzxopc8L+wUwVg6cKWqi49UbKzMkwhAgUmt+0uJBtUW/TpjDhuWz+/MrzQ==&uN90=Wv0xlDNhhL
	20210812GLL_pdf.exe	Get hash	malicious	Browse	- www.ptkvoice.com/zrmt/?iZG=ctrCe2mnbuueYdlFChD4/ovjSbegx+fsxvMp2r+zhNsJlDd5OS/NhYw/p1KrtWBZElqC&4hVP=u2JPvzz8
	SWIFT001411983HNK.exe	Get hash	malicious	Browse	- www.shortexts.com/epns/?6lS0=dI3Yf9uTZTAbXCF6BbS/gogk1F2wKsRWmNO0p//NNyZfeVIkQt6IT+pUp6SqlYDuC11l&hVW=UjWlVXm0fTLtynY

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• www.alldaazz.com/maw9/?0V0hlZ=XWXsKoTGIm4uHXuwUxI2SWJVNAtoSeX/AD8kJREhnqN4l6QppauIxxnj5QSnUcXcVB4L&OVolp8=AZ9lQ6QHS8EdPrG0
	L0CzpAvZC0.docm	Get hash	malicious	Browse	• wnc2sod.com/jivo/neky.php?l=wosam7.cab
	http://victoriascrets.com	Get hash	malicious	Browse	• victoriascrets.com/
	Nuevo orden.exe	Get hash	malicious	Browse	• www.bdcamp.com/fs8/?Rbd=M6AtZDq0P&sZ8p=NOEji/Y2mGsbH23/deqaMT6z03hOleRIA9g6aYtYA7Z0zE2bvyN9F2FNz4vb/LyrvrKV
	http://cootewie.com	Get hash	malicious	Browse	• cootewie.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com	PO11232021.xlsx	Get hash	malicious	Browse	• 54.159.173.74
	3543lZhfll.exe	Get hash	malicious	Browse	• 54.211.95.91

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	2HFJezUWHA.exe	Get hash	malicious	Browse	• 52.20.78.240
	QZLQkiS4nj.exe	Get hash	malicious	Browse	• 52.20.78.240
	Jx35I5pwgd	Get hash	malicious	Browse	• 54.167.122.21
	meerkat.x86	Get hash	malicious	Browse	• 34.228.218.187
	invoice copy.pdf.exe	Get hash	malicious	Browse	• 52.200.197.31
	mal1.html	Get hash	malicious	Browse	• 23.20.158.212
	oQANZnrt9d	Get hash	malicious	Browse	• 54.34.104.203
	KWDww9OWgh	Get hash	malicious	Browse	• 44.207.141.47
	TwikaSb2s6	Get hash	malicious	Browse	• 54.204.237.164
	TWb3IVgBOQ.exe	Get hash	malicious	Browse	• 35.169.3.110
	sora.x86	Get hash	malicious	Browse	• 54.62.131.219
	a.dll	Get hash	malicious	Browse	• 44.200.20.85
	New Order778880.exe	Get hash	malicious	Browse	• 3.209.180.95
	B67M2Q6NeK	Get hash	malicious	Browse	• 44.194.145.165
	c0az1l4js3001lsk4xd9n.arm7-20211124-0850	Get hash	malicious	Browse	• 44.207.229.114
	c0az1l4js3001lsk4xd9n.arm-20211124-0850	Get hash	malicious	Browse	• 34.231.85.166
	0617_1876522156924.doc	Get hash	malicious	Browse	• 54.91.59.199
	C594188774A2D72B774ACA96EB096C493DBE5C9B599BE.exe	Get hash	malicious	Browse	• 54.83.52.76
	x86_64-20211124-0649	Get hash	malicious	Browse	• 54.210.131.199
	jLvGTP8xik	Get hash	malicious	Browse	• 34.235.189.214
TRELLIAN-AS-APTrellianPtyLimitedAU	piPvSLcFXV.exe	Get hash	malicious	Browse	• 103.224.212.220
	Env#U00edo diciembre.exe	Get hash	malicious	Browse	• 103.224.182.253
	IAENMAI.xlsx	Get hash	malicious	Browse	• 103.224.182.210
	SecuriteInfo.com.Trojan.Siggen15.46065.1499.exe	Get hash	malicious	Browse	• 103.224.182.246
	MDXAR5336e.exe	Get hash	malicious	Browse	• 103.224.212.222
	7OjVU04f8q.exe	Get hash	malicious	Browse	• 103.224.212.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rfq.exe	Get hash	malicious	Browse	• 103.224.212.220
	Scan-Copy.doc	Get hash	malicious	Browse	• 103.224.182.242
	11#U6708 16#U65e5 BL #U505a#U6cd5 SO NO J624 - #U9577#U5f91ISF DETAILS SO J624.exe	Get hash	malicious	Browse	• 103.224.212.219
	PO AMO 8100045923.xlsx	Get hash	malicious	Browse	• 103.224.212.221
	Company Profile.exe	Get hash	malicious	Browse	• 103.224.212.219
	XL9048621.exe	Get hash	malicious	Browse	• 103.224.182.210
	goGZ1Tg0WT.exe	Get hash	malicious	Browse	• 103.224.212.220
	BwJriVGrt5.exe	Get hash	malicious	Browse	• 103.224.182.208
	RQF_190011234.doc	Get hash	malicious	Browse	• 103.224.212.221
	HIRE SOA NOV.exe	Get hash	malicious	Browse	• 103.224.212.219
	RFQ - JAKOB SELMER_pdf.exe	Get hash	malicious	Browse	• 103.224.212.220
	Quote request.exe	Get hash	malicious	Browse	• 103.224.212.220
	Purchase Order - 10,000MT.exe	Get hash	malicious	Browse	• 103.224.212.221
	copy.exe	Get hash	malicious	Browse	• 103.224.182.242

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HkE0tD0g4NXKJfy.exe.log	
Process:	C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A42346 85
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.841777584881155
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:	HkE0tD0g4NXKJfy.exe
File size:	446976
MD5:	fcc2d1cda8d3989feca9c5f5f900e164
SHA1:	075de723df172cc93c537d5472ad8025f192ddc8
SHA256:	77e1c24ecfa1d339f61b4b8011690425fa0038b3fe32761f5ce8b3126c28c5ad
SHA512:	25f45048ee6bc9164177634d6e4b9f4d3aac06d4d305aa25c16eaf8cf2169767f86cd2879ddabe2e49d8fd38b0a50e115b1735da5a4600ec8c1e243bff2b4863
SSDEEP:	12288:wdmXM0WMbeBBYMtWpeUjxU9sQ+WYU1y1wjlvixBFm:wdoM0yGptdU9+WYkvjlvi1
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L...-O.a.............0.............B.... ....@.. ....@............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46e642
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:	0x619F4F2D [Thu Nov 25 08:54:05 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
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	0x6c658	0x6c800	False	0.883170272897	data	7.85414523612	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x5fc	0x600	False	0.436848958333	data	4.2146833829	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x72000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-15:09:09.126288	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49766	34.102.136.180	192.168.2.3
11/25/21-15:09:14.229963	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49786	80	192.168.2.3	34.102.136.180
11/25/21-15:09:14.229963	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49786	80	192.168.2.3	34.102.136.180
11/25/21-15:09:14.229963	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49786	80	192.168.2.3	34.102.136.180
11/25/21-15:09:14.348176	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49786	34.102.136.180	192.168.2.3
11/25/21-15:09:19.479118	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49792	80	192.168.2.3	142.250.203.115
11/25/21-15:09:19.479118	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49792	80	192.168.2.3	142.250.203.115
11/25/21-15:09:19.479118	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49792	80	192.168.2.3	142.250.203.115
11/25/21-15:09:36.061017	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49812	34.102.136.180	192.168.2.3
11/25/21-15:09:45.250397	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
11/25/21-15:10:15.460524	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49821	34.102.136.180	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 15:09:08.834608078 CET	192.168.2.3	8.8.8.8	0x23a1	Standard query (0)	www.platinumcredit.net	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:14.145761967 CET	192.168.2.3	8.8.8.8	0x8897	Standard query (0)	www.151motors.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:19.383676052 CET	192.168.2.3	8.8.8.8	0x93b8	Standard query (0)	www.suepersoldiers.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:25.058619976 CET	192.168.2.3	8.8.8.8	0xe941	Standard query (0)	www.thefullfledged.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:30.115839005 CET	192.168.2.3	8.8.8.8	0xd6b	Standard query (0)	www.arsels.info	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:35.863133907 CET	192.168.2.3	8.8.8.8	0xf03e	Standard query (0)	www.electricatrick.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:41.107296944 CET	192.168.2.3	8.8.8.8	0xbdc7	Standard query (0)	www.jakital.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:42.128709078 CET	192.168.2.3	8.8.8.8	0xbdc7	Standard query (0)	www.jakital.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:43.175431967 CET	192.168.2.3	8.8.8.8	0xbdc7	Standard query (0)	www.jakital.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 15:10:05.613094091 CET	192.168.2.3	8.8.8.8	0x6d29	Standard query (0)	www.jakital.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:09.370842934 CET	192.168.2.3	8.8.8.8	0xa6f8	Standard query (0)	www.xcgtsret.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:15.279592037 CET	192.168.2.3	8.8.8.8	0xf205	Standard query (0)	www.vupeliquid.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:20.474148035 CET	192.168.2.3	8.8.8.8	0xf7cb	Standard query (0)	www.nbtianzhou.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:09:08.901595116 CET	8.8.8.8	192.168.2.3	0x23a1	No error (0)	www.platinumcredit.net	platinumcredit.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:09:08.901595116 CET	8.8.8.8	192.168.2.3	0x23a1	No error (0)	platinumcredit.net		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:14.206563950 CET	8.8.8.8	192.168.2.3	0x8897	No error (0)	www.151motors.com	151motors.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:09:14.206563950 CET	8.8.8.8	192.168.2.3	0x8897	No error (0)	151motors.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:19.459450960 CET	8.8.8.8	192.168.2.3	0x93b8	No error (0)	www.sueper soldiers.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:09:19.459450960 CET	8.8.8.8	192.168.2.3	0x93b8	No error (0)	ghs.googlehosted.com		142.250.203.115	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:25.097635031 CET	8.8.8.8	192.168.2.3	0xe941	Name error (3)	www.thefullfledged.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:30.372935057 CET	8.8.8.8	192.168.2.3	0xd6b	No error (0)	www.arsels.info		103.224.212.219	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:35.918409109 CET	8.8.8.8	192.168.2.3	0xf03e	No error (0)	www.electricatrick.com	electricatrick.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:09:35.918409109 CET	8.8.8.8	192.168.2.3	0xf03e	No error (0)	electricatrick.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:43.262866020 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	www.jakital.com	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:09:43.262866020 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		52.204.216.132	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:43.262866020 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		54.164.248.48	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:45.250235081 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	www.jakital.com	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:09:45.250235081 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		52.204.216.132	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:45.250235081 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		54.164.248.48	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:09:45.317536116 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	www.jakital.com	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:09:45.317536116 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		52.204.216.132	A (IP address)	IN (0x0001)
Nov 25, 2021 15:09:45.317536116 CET	8.8.8.8	192.168.2.3	0xbdc7	No error (0)	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		54.164.248.48	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:05.650708914 CET	8.8.8.8	192.168.2.3	0x6d29	No error (0)	www.jakital.com	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:10:05.650708914 CET	8.8.8.8	192.168.2.3	0x6d29	No error (0)	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		52.204.216.132	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:05.650708914 CET	8.8.8.8	192.168.2.3	0x6d29	No error (0)	AutoScale-HDRedirect-ALB-1-1859847625.us-east-1.elb.amazonaws.com		54.164.248.48	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:10.272214890 CET	8.8.8.8	192.168.2.3	0xa6f8	Server failure (2)	www.xcgtsret.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:15.319477081 CET	8.8.8.8	192.168.2.3	0xf205	No error (0)	www.vupeliquid.com	vupeliquid.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:10:15.319477081 CET	8.8.8.8	192.168.2.3	0xf205	No error (0)	vupeliquid.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.platinumcredit.net
- www.151motors.com
- www.suepersoldiers.com
- www.arsels.info
- www.electricatrick.com
- www.vupeliquid.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49766	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:09:08.945138931 CET	1731	OUT	GET /sh5d/?Yv=hy4EQ9RQ8H0Qmf+V5oZYawTzVdNi6YgEsN2g+zlr8kWBt8RwCZI+yMGy7WuYiu2G3qgy&8pZ=MFQX HTTP/1.1 Host: www.platinumcredit.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:09:09.126287937 CET	1734	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 14:09:09 GMT Content-Type: text/html Content-Length: 275 ETag: "618be73d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body><h1>Access Forbidden</h1></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49786	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:09:14.229963064 CET	1779	OUT	GET /sh5d/?Yv=KHnqZ0TbjHhhriSsr4IC2tQHFpsEpNX6XKtcehIZDPMVzpPTFiaMMZSG67rbMC0Gdpxx&8pZ=MFQX HTTP/1.1 Host: www.151motors.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:09:14.348176003 CET	1780	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 14:09:14 GMT Content-Type: text/html Content-Length: 275 ETag: "618be75c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body><h1>Access Forbidden</h1></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49792	142.250.203.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:09:19.479118109 CET	6789	OUT	GET /sh5d/?Yv=SDhgbwSt5mB4DODrBIecU0Cn9nI1MHSsH0Hazkrlv9wpSquk3LdmspAinMLs2LJY3gHa&8pZ=MFQX HTTP/1.1 Host: www.suepersoldiers.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:09:20.481894016 CET	6790	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 14:09:20 GMT Expires: Thu, 25 Nov 2021 14:19:20 GMT Cache-Control: public, max-age=600 ETag: "QUrYJA" X-Cloud-Trace-Context: e9bf4e2176d1e4f430f08354d7ed8296 Content-Type: text/html Transfer-Encoding: chunked Server: Google Frontend Connection: close Data Raw: 33 65 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 3e 3c 74 69 74 6c 65 3e 53 75 65 70 65 72 20 53 6f 6c 64 69 65 72 73 3c 2f 74 69 74 6c 65 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 52 6f 62 6f 74 6f 3a 31 30 30 2c 33 30 30 2c 34 30 30 2c 35 30 30 2c 37 30 30 2c 39 30 30 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 2e 6a 73 64 65 6c 69 76 72 2e 6e 65 74 2f 6e 70 6d 2f 40 6d 64 69 2f 66 6f 6e 74 40 6c 61 74 65 73 74 2f 63 73 73 2f 6d 61 74 65 72 69 61 6c 64 65 73 69 67 6e 69 63 6f 6e 73 2e 6d 69 6e 2e 63 73 73 22 3e 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 63 73 73 2f 63 68 75 6e 6b 2d 76 65 6e 64 6f 72 73 2e 38 61 63 63 64 31 63 35 2e 63 73 73 22 20 72 65 6c 3d 22 70 72 65 6c 6f 61 64 22 20 61 73 3d 22 73 74 79 6c 65 22 3e 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 6a 73 2f 61 70 70 2e 39 30 39 30 37 31 32 38 2e 6a 73 22 20 72 65 6c 3d 22 70 72 65 6c 6f 61 64 22 20 61 73 3d 22 73 63 72 69 70 74 22 3e 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 6a 73 2f 63 68 75 6e 6b 2d 76 65 6e 64 6f 72 73 2e 61 66 38 38 30 39 32 37 2e 6a 73 22 20 72 65 6c 3d 22 70 72 65 6c 6f 61 64 22 20 61 73 3d 22 73 63 72 69 70 74 22 3e 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 63 73 73 2f 63 68 75 6e 6b 2d 76 65 6e 64 6f 72 73 2e 38 61 63 63 64 31 63 35 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 6e 6f 73 63 72 69 70 74 3e 3c 73 74 72 6f 6e 67 3e 57 65 27 72 65 20 73 6f 72 72 79 20 62 75 74 20 53 75 65 70 65 72 20 53 6f 6c 64 69 65 72 73 20 64 6f 65 73 6e 27 74 20 77 6f 72 6b 20 70 72 6f 70 65 72 6c 79 20 77 69 74 68 6f 75 74 20 4a 61 76 61 53 63 72 69 70 74 20 65 6e 61 62 6c 65 64 2e 20 50 6c 65 61 73 65 20 65 6e 61 62 6c 65 20 69 74 20 74 6f 20 63 6f 6e 74 69 6e 75 65 2e 3c 2f 73 74 72 6f 6e 67 3e 3c 2f 6e 6f 73 63 72 69 70 74 3e 3c 64 69 76 20 69 64 3d 22 61 70 70 22 3e 3c 2f 64 69 76 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 6a 73 2f 63 68 75 6e 6b 2d 76 65 6e 64 6f 72 73 2e 61 66 38 38 30 39 32 37 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 6a 73 2f 61 70 70 2e 39 30 39 30 37 31 32 38 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 3ef<!DOCTYPE html><html lang="en"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1"><link rel="icon" href="/favicon.ico"><title>Sueper Soldiers</title><link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,300,400,500,700,900"><link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/@mdi/font@latest/css/materialdesignicons.min.css"><link href="/css/chunk-vendors.8accd1c5.css" rel="preload" as="style"><link href="/js/app.90907128.js" rel="preload" as="script"><link href="/js/chunk-vendors.af880927.js" rel="preload" as="script"><link href="/css/chunk-vendors.8accd1c5.css" rel="stylesheet"></head><body><noscript><strong>We're sorry but Sueper Soldiers doesn't work properly without JavaScript enabled. Please enable it to continue.</strong></noscript><div id="app"></div><script src="/js/chunk-vendors.af880927.js"></script><script src="/js/app.90907128.js"></script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49794	103.224.212.219	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:09:30.601727009 CET	7145	OUT	GET /sh5d/?Yv=U9Dn+H6I1oLCGiFi1oW/bg7Rnic0zjRPtt9AMGb5MRiLdOF7LfbhYF1T4mwo8MTrEy0Q&8pZ=MFQX HTTP/1.1 Host: www.arsels.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:09:30.842940092 CET	7146	IN	HTTP/1.1 302 Found Date: Thu, 25 Nov 2021 14:09:30 GMT Server: Apache/2.4.25 (Debian) Set-Cookie: __tad=1637849370.3647175; expires=Sun, 23-Nov-2031 14:09:30 GMT; Max-Age=315360000 Location: http://ww25.arsels.info/sh5d/?Yv=U9Dn+H6I1oLCGiFi1oW/bg7Rnic0zjRPtt9AMGb5MRiLdOF7LfbhYF1T4mwo8MTrEy0Q&8pZ=MFQX&subid1=20211126-0109-303d-a829-871fbc9656f2 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49812	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:09:35.941904068 CET	7185	OUT	GET /sh5d/?Yv=bH0MuGY0n47F1S4kOvzCBL0/mw6YL+7138CmEb6WqYz18csJYDgpNmReh/JvI3nBbY8S&8pZ=MFQX HTTP/1.1 Host: www.electricatrick.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:09:36.061017036 CET	7187	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 14:09:36 GMT Content-Type: text/html Content-Length: 275 ETag: "6192576c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body><h1>Access Forbidden</h1></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49821	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:10:15.342689991 CET	7206	OUT	GET /sh5d/?Yv=Pdn0Hokg7Q3B7dDVtUX5QMohVVbqJZ0HrhWfxUy6sRCS+GjM4sZ5xKohcZ81Ep8iPYLe&8pZ=MFQX HTTP/1.1 Host: www.vupeliquid.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:10:15.460524082 CET	7207	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 14:10:15 GMT Content-Type: text/html Content-Length: 275 ETag: "6192576d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body><h1>Access Forbidden</h1></body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: HkE0tD0g4NXKJfy.exe PID: 5624 Parent PID: 5256

General

Start time:	15:08:07
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe"
Imagebase:	0xc10000
File size:	446976 bytes
MD5 hash:	FCC2D1CDA8D3989FECA9C5F5F900E164
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.291957293.000000000314B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.291856624.0000000003081000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.292187512.000000000408D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.292187512.000000000408D000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.292187512.000000000408D000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.292465648.00000000042A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.292465648.00000000042A7000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.292465648.00000000042A7000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: HkE0tD0g4NXKJfy.exe PID: 3336 Parent PID: 5624

General

Start time:	15:08:10
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe
Imagebase:	0xe60000
File size:	446976 bytes
MD5 hash:	FCC2D1CDA8D3989FECA9C5F5F900E164
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: 00000007.00000002.346581658.0000000001450000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.346581658.0000000001450000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.346581658.0000000001450000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.346764994.0000000001880000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.346764994.0000000001880000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.346764994.0000000001880000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.346144380.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.346144380.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.346144380.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.289531768.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.289531768.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.289531768.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.290051864.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.290051864.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.290051864.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 3336

General

Start time:	15:08:13
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
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: 0000000A.00000000.323615980.000000000F7EA000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.323615980.000000000F7EA000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.323615980.000000000F7EA000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: msdt.exe PID: 5960 Parent PID: 3352

General

Start time:	15:08:34
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x1b0000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 0000000D.00000002.554339019.0000000002D00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.554339019.0000000002D00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.554339019.0000000002D00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.551703779.0000000000970000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.551703779.0000000000970000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.551703779.0000000000970000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.553715961.0000000002C00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.553715961.0000000002C00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.553715961.0000000002C00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 5904 Parent PID: 5960

General

Start time:	15:08:39
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\HkE0tD0g4NXKJfy.exe"
Imagebase:	0xd80000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 6108 Parent PID: 5904

General

Start time:	15:08:40
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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

Code Analysis