ID: 385277
Sample Name:
#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe
Cookbook: default.jbs
Time: 09:30:08
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

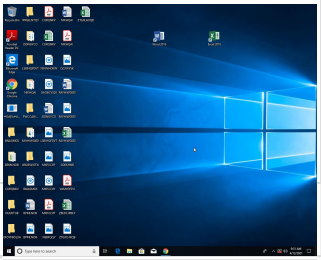
Analysis Report #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#U…

Overview

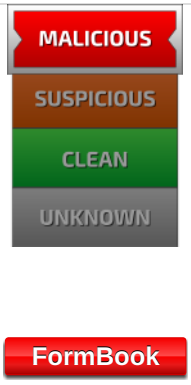
General Information

Sample Name:	#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe
Analysis ID:	385277
MD5:	525cb22afe0244e.
SHA1:	df33a4a91f50e49..
SHA256:	bcbdc1722d82cfd..
Tags:	exe Formbook geo KOR
Infos:	

Most interesting Screenshot:



Detection



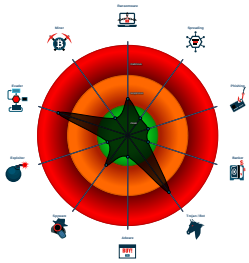
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Antivirus or Machine Learning detec…
- Binary contains a suspicious time st…

Classification



Startup

- **System is w10x64**
- #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe (PID: 6476 cmdline: 'C:\Users\user\Desktop\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe' MD5: 525CB22AFE0244E45B2831B243B27A68)
  - #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe (PID: 6616 cmdline: {path} MD5: 525CB22AFE0244E45B2831B243B27A68)
  - #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe (PID: 6632 cmdline: {path} MD5: 525CB22AFE0244E45B2831B243B27A68)
  - #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe (PID: 6644 cmdline: {path} MD5: 525CB22AFE0244E45B2831B243B27A68)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.visitmatchgo.com/duy/"
  ],
  "decoy": [
    "tychzh.net",
    "seafoodrambler.com",
    "sustainablyoutdoors.com",
    "ngisolomba.club",
    "pocee.com",
    "toshaliusa.com",
    "authenticpickleball.com",
    "2jm.guru",
    "site4v.com",
    "earlywarningsigns.com",
    "freekwennekers.com",
    "noelgift.store",
    "timaloney.com",
    "scotlandluxurylodges.com",
    "xevroruwf.icu",
    "ideasforgoodcourse.com",
    "feederscup.com",
    "kabutostrength.com",
    "studiomileend.com",
    "restaurantenelia.com",
    "kentbranding.company",
    "whitelinen.house",
    "mighty.zone",
    "bigsky3percent.com",
    "satelliteshows.com",
    "hlbrock.com",
    "xn--tssla-gra.com",
    "theholisticmix.com",
    "therealdmu.com",
    "lentiacontattoeshop.com",
    "uhejcjew.icu",
    "casnop.com",
    "lavisheclothiers.com",
    "topelevenhackcheatz.com",
    "monterklime.com",
    "fanoosbattery.com",
    "laramsmatter.com",
    "morrolion.com",
    "itstime4recess.com",
    "leeurgentcare.com",
    "panamienne.com",
    "implementbiosegurityoneline.com",
    "roseyogacoach.com",
    "domennyarendi19.net",
    "antsclassic.win",
    "soredecoraciones.com",
    "thelittlejetscompany.com",
    "culturasoft.net",
    "aajfw.xyz",
    "thedreamdistrict.com",
    "gmgdr.com",
    "releasement.solutions",
    "ditrdan.com",
    "ecoshoplanet.com",
    "boblikescock.com",
    "cotizalo.online",
    "gulastivbgone.xyz",
    "quelastimamiguelito.com",
    "tld-qa.com",
    "14pro.com",
    "michaeljoycetennis.com",
    "petrickpetmarket.xyz",
    "agilearccreations.com",
    "281as39.xyz"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.337974724.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.337974724.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.337974724.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.338606384.0000000004249000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.338606384.0000000004249000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1482e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148562:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x174908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x174b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x154085:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1806a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x153b71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x180191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x154187:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1807a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1542ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x18091f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x148f7a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x17559a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x152dec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x17f40c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x149c73:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x176293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x159d27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x186347:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x15ad2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 2 entries				

Unpacked PEs

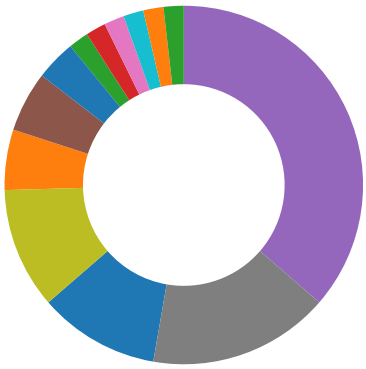
Source	Rule	Description	Author	Strings
5.2.#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
5.2.#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
5.2.#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$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

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Stealing of Sensitive Information:

Yara detected FormBook

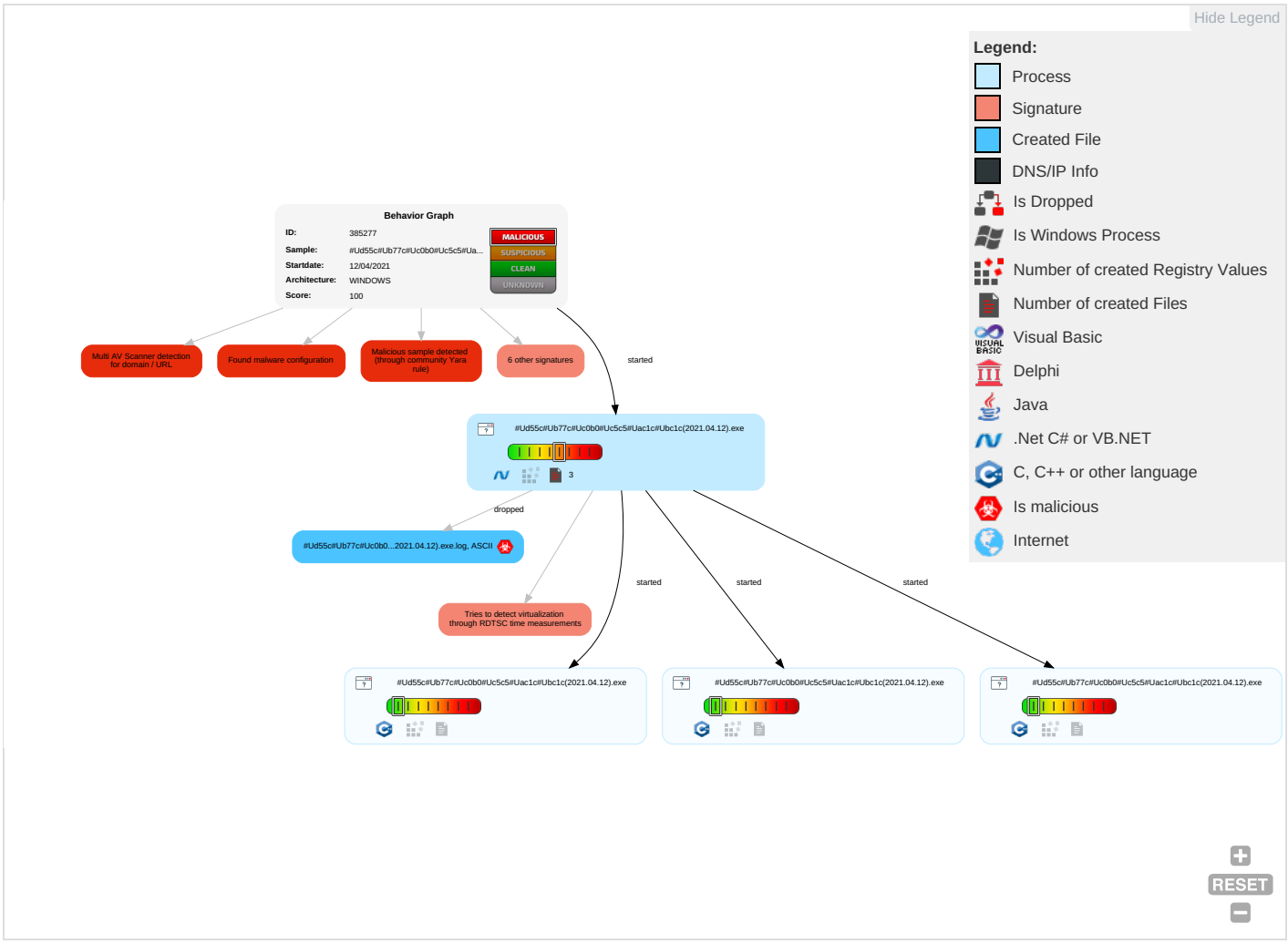
Remote Access Functionality:

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	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Information Discovery 1 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade 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
#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe	27%	Virustotal		Browse
#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.Woreflint	
#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.visitmatchgo.com/duy/	7%	Virustotal		Browse
www.visitmatchgo.com/duy/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.visitmatchgo.com/duy/	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	low

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385277
Start date:	12.04.2021
Start time:	09:30:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).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:	8
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@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 1%) • Quality average: 82% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe

Simulations

Behavior and APIs

Time	Type	Description
09:30:58	API Interceptor	1x Sleep call for process: #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.log	
Process:	C:\Users\user\Desktop\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.log	
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):	7.88721653299409
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe
File size:	698880
MD5:	525cb22afe0244e45b2831b243b27a68
SHA1:	df33a4a91f50e49ee7c3283b1022024fca7ceade
SHA256:	bcbdc1722d82cfdd00d6748654937dd6e79b81661df159e a9387d61f3ed38034
SHA512:	369ccf65d7a03a981c13a223e67ae02665cfd41fdacfbb9 c5ab300c61556d0161938e8baa32631da7425e14ac344c 0e34bd71b56dcc59e33703b625d20b72d01
SSDEEP:	12288:eUA8Dpprq/7mz98ARu519pEpCPXD3XkeXxSHnob0agtjty2PouxcM1:eUA8iy5NO1YGnzQZnyIL
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....J................0................. ....@.. ....@...............................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4abf1e
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:	0xDE084AFD [Fri Jan 16 09:57:17 2088 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xabecc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x5f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xabeb0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa9f24	0xaa000	False	0.903818646599	data	7.89372694825	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x5f8	0x600	False	0.438802083333	data	4.22543998316	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xae000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xac090	0x366	data		
RT_MANIFEST	0xac408	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Integra Wealth
Assembly Version	1.8.9.10
InternalName	u4tB.exe
FileVersion	1.9.1.0
CompanyName	Integra Wealth
LegalTrademarks	
Comments	
ProductName	ReplacementFallback
ProductVersion	1.9.1.0
FileDescription	ReplacementFallback
OriginalFilename	u4tB.exe

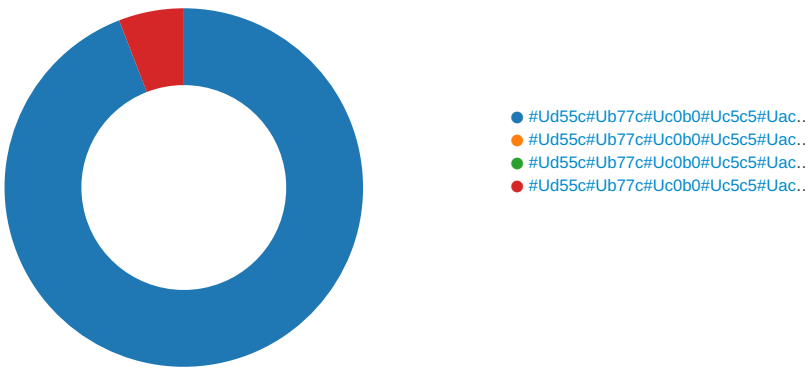
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe PID: 6476 Parent PID: 5964

General

Start time:	09:30:57
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe'
Imagebase:	0xd50000
File size:	698880 bytes
MD5 hash:	525CB22AFE0244E45B2831B243B27A68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.338606384.0000000004249000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.338606384.0000000004249000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.338606384.0000000004249000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEDCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEDCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E1EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD21B4F	ReadFile

Analysis Process: #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe PID: 6616 Parent PID: 6476

General

Start time:	09:31:01
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2a0000
File size:	698880 bytes
MD5 hash:	525CB22AFE0244E45B2831B243B27A68

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

Analysis Process: #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe PID: 6632 Parent PID: 6476

General

Start time:	09:31:01
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1d0000
File size:	698880 bytes
MD5 hash:	525CB22AFE0244E45B2831B243B27A68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: #Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe PID: 6644 Parent PID: 6476

General

Start time:	09:31:02
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\#Ud55c#Ub77c#Uc0b0#Uc5c5#Uac1c#Ubc1c(2021.04.12).exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbe0000
File size:	698880 bytes
MD5 hash:	525CB22AFE0244E45B2831B243B27A68
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: 00000005.00000002.337974724.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.337974724.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.337974724.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Disassembly

Code Analysis