

JOeSandbox Cloud BASIC



ID: 552852

Sample Name:

Fp4grWelSC.exe

Cookbook: default.jbs

Time: 20:21:28

Date: 13/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Fp4grWelSC.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: FormBook	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	6
Sigma Overview	7
Jbx Signature Overview	7
AV Detection:	7
Networking:	7
E-Banking Fraud:	7
System Summary:	7
Data Obfuscation:	7
Hooking and other Techniques for Hiding and Protection:	7
Malware Analysis System Evasion:	7
HIPS / PFW / Operating System Protection Evasion:	7
Stealing of Sensitive Information:	8
Remote Access Functionality:	8
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
Contacted IPs	11
General Information	11
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASN	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	14
Data Directories	14
Sections	14
Resources	14
Imports	14
Version Infos	14
Network Behavior	14
Code Manipulations	14
Statistics	14
Behavior	14
System Behavior	14
Analysis Process: Fp4grWelSC.exe PID: 7132 Parent PID: 5332	14
General	14
File Activities	15
File Created	15
File Written	15
File Read	15
Analysis Process: Fp4grWelSC.exe PID: 6436 Parent PID: 7132	15
General	15
File Activities	16

File Read	16
Analysis Process: explorer.exe PID: 3424 Parent PID: 6436	16
General	16
Analysis Process: autochk.exe PID: 6860 Parent PID: 3424	17
General	17
Analysis Process: cmd.exe PID: 7036 Parent PID: 3424	17
General	17
File Activities	18
File Read	18
Analysis Process: cmd.exe PID: 7080 Parent PID: 7036	18
General	18
File Activities	18
Analysis Process: conhost.exe PID: 7020 Parent PID: 7080	18
General	18
Analysis Process: explorer.exe PID: 5396 Parent PID: 5256	19
General	19
File Activities	19
Registry Activities	19
Analysis Process: explorer.exe PID: 3460 Parent PID: 576	19
General	19
File Activities	19
Registry Activities	19
Disassembly	19
Code Analysis	19

Windows Analysis Report Fp4grWelSC.exe

Overview

General Information

Sample Name:	Fp4grWelSC.exe
Analysis ID:	552852
MD5:	0e99d13aafcc5e8..
SHA1:	6573c9dd229e50..
SHA256:	a15402c5f869a1c..
Tags:	exe
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

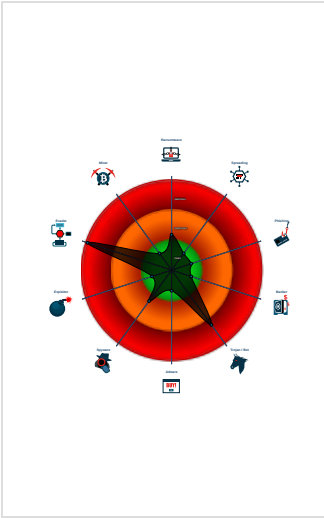
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through ...
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an...
- Tries to detect sandboxes and other...
- Machine Learning detection for samp...
- Self deletion via cmd delete
- .NET source code contains potentia...

Classification



Process Tree

- System is w10x64
- Fp4grWelSC.exe (PID: 7132 cmdline: "C:\Users\user\Desktop\Fp4grWelSC.exe" MD5: 0E99D13AAFCC5E8FADC45D8B85336D9B)
 - Fp4grWelSC.exe (PID: 6436 cmdline: C:\Users\user\Desktop\Fp4grWelSC.exe MD5: 0E99D13AAFCC5E8FADC45D8B85336D9B)
 - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 - autochk.exe (PID: 6860 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
 - cmd.exe (PID: 7036 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - cmd.exe (PID: 7080 cmdline: /c del "C:\Users\user\Desktop\Fp4grWelSC.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - conhost.exe (PID: 7020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - explorer.exe (PID: 5396 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 - explorer.exe (PID: 3460 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- cleanup

Malware Configuration

Threatname: FormBook

```

{
  "C2 list": [
    "www.safetyeats.asia/pnug/"
  ],
  "decoy": [
    "natureate.com",
    "ita-pots.website",
    "sucohansmushroom.com",
    "produrielrosen.com",
    "gosystemupdatenow.online",
    "jiskra.art",
    "janwiench.com",
    "norfolkfoodhall.com",
    "iloveaddictss.com",
    "pogozip.com",
    "buyinstapva.com",
    "teardirectionfreedom.xyz",
    "0205168.com",
    "apaixonadosporpugs.online",
    "jawscoinc.com",
    "crafter.quest",
    "wikipedianow.com",
    "radiopuls.net",
    "kendama-co.com",
    "goodstudycanada.com",
    "huzhoucs.com",
    "asinment.com",
    "fuchsundrudolph.com",
    "arthurenathalia.com",
    "globalcosmeticsstudios.com",
    "brandrackley.com",
    "freemanhub.one",
    "utserver.online",
    "fullspecter.com",
    "wshowcase.com",
    "airjordanshoes-retro.com",
    "linguimatics.com",
    "app-verlengen.icu",
    "singpost.red",
    "j4.claims",
    "inoteapp.net",
    "jrdautomotive LLC.com",
    "xn--beaupre-6xa.com",
    "mypolicyportal.net",
    "wdgjdhpg.com",
    "anshulindia.com",
    "m981070.com",
    "vertentebike.com",
    "claim-available.com",
    "buyfudgybombs.com",
    "adfnapoli.com",
    "blackfuid.com",
    "clambakedelivered.info",
    "marketingworksonhold.com",
    "xvyj.top",
    "richardsonsfine.com",
    "gurimix.com",
    "dorchop.com",
    "mauigrowgreencoffee.net",
    "juzytuu.xyz",
    "pokorny.industries",
    "floridapermitsolutions.com",
    "right-on-target-store.com",
    "ynaire.com",
    "nextpar.com",
    "disdrone.com",
    "fruitfulvinebirth.com",
    "africanfairytale.com",
    "leisuresabah.com"
  ]
}

```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.939516998.00000000007C 0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.939516998.00000000007C 0000.00000040.00020000.sdmf	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x8608:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x89a2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146b5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x141a1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147b7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1492f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93ba:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1341c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa132:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19ba7:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac4a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.939516998.00000000007C 0000.00000040.00020000.sdmf	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> 0x16ad9:\$sqlite3step: 68 34 1C 7B E1 0x16bec:\$sqlite3step: 68 34 1C 7B E1 0x16b08:\$sqlite3text: 68 38 2A 90 C5 0x16c2d:\$sqlite3text: 68 38 2A 90 C5 0x16b1b:\$sqlite3blob: 68 53 D8 7F 8C 0x16c43:\$sqlite3blob: 68 53 D8 7F 8C
00000004.00000000.686284909.0000000000400000.00000 040.00000001.sdmf	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000000.686284909.0000000000400000.00000 040.00000001.sdmf	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x8608:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x89a2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146b5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x141a1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147b7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1492f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93ba:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1341c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa132:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19ba7:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac4a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.Fp4grWelSC.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.Fp4grWelSC.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x8608:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x89a2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146b5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x141a1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147b7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1492f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93ba:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1341c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa132:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19ba7:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac4a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.Fp4grWelSC.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> 0x16ad9:\$sqlite3step: 68 34 1C 7B E1 0x16bec:\$sqlite3step: 68 34 1C 7B E1 0x16b08:\$sqlite3text: 68 38 2A 90 C5 0x16c2d:\$sqlite3text: 68 38 2A 90 C5 0x16b1b:\$sqlite3blob: 68 53 D8 7F 8C 0x16c43:\$sqlite3blob: 68 53 D8 7F 8C
4.0.Fp4grWelSC.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.Fp4grWelSC.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x7808:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x7ba2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x138b5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x133a1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x139b7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x13b2f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x85ba:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1261c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x9332:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x18da7:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x19e4a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 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

Antivirus detection for URL or domain

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)

Data Obfuscation:



.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:



Self deletion via cmd delete

Malware Analysis System Evasion:



Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:



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 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 5 1 2	Access Token Manipulation 1	Security Account Manager	Security Software Discovery 2 6 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 4 1	LSA Secrets	Virtualization/Sandbox Evasion 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 5 1 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 2 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
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	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Fp4grWelSC.exe	30%	Virustotal		Browse
Fp4grWelSC.exe	39%	ReversingLabs	Win32.Trojan.Generic	
Fp4grWelSC.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.Fp4grWelSC.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.Fp4grWelSC.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.Fp4grWelSC.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.Fp4grWelSC.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comldW	0%	Avira URL Cloud	safe	
http://en.wV	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.comas	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnew	0%	Avira URL Cloud	safe	
www.safeyeats.asia/pnug/	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://crl.v	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.safeyeats.asia/pnug/	true	<ul style="list-style-type: none"> Avira URL Cloud: malware 	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552852
Start date:	13.01.2022
Start time:	20:21:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fp4grWeISC.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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/1@0/0
EGA Information:	<ul style="list-style-type: none">• Successful, ratio: 66.7%
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 23.7% (good quality ratio 21.1%)• Quality average: 67.3%• Quality standard deviation: 33.4%
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:22:31	API Interceptor	1x Sleep call for process: Fp4grWeISC.exe modified
20:23:43	API Interceptor	172x Sleep call for process: explorer.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\Fp4grWelSC.exe.log	
Process:	C:\Users\user\Desktop\Fp4grWelSC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFHKHkoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKHqNoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	true
Reputation:	moderate, 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\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\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\1f1d8480152e0da9a60ad49c6d16a3b6d\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):	7.294974785296935
TrID:	<ul style="list-style-type: none">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:	Fp4grWelSC.exe
File size:	595968
MD5:	0e99d13aafcc5e8fad45d8b85336d9b
SHA1:	6573c9dd229e50981aa24128ad02a07e99805369
SHA256:	a15402c5f869a1c02421742c27dd71c2448bb037d391a6bf130be06b2f976e2f
SHA512:	d2c22cff7ad0e8ea73b4d6a82f732d5d4f10033598040d545f00711d5a9c10c2d78e5c5aa17c8cacf9434e361f4b947a33c4849e800e2f3df7b73245ecd69d5a
SSDEEP:	12288:IK777777777777YPLgd5c/MhOk1nFhLuxbW54Tz/9KOGKTZZtqlQ2x:IK777777777777YMd5cmOksxOeBEQjD
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.PE..L....%a.....0..B.....^a.....@.....@.....@.....

File Icon

	
Icon Hash:	d2fafaf2f2dadac4

Static PE Info

General	
Entrypoint:	0x46615e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E025D6 [Thu Jan 13 13:15:02 2022 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	0x64164	0x64200	False	0.881544553683	data	7.74639201184	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x2d104	0x2d200	False	0.320323320637	data	5.73852496041	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x96000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Fp4grWelSC.exe PID: 7132 Parent PID: 5332

General

Start time:	20:22:21
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\Fp4grWelSC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Fp4grWelSC.exe"
Imagebase:	0x370000
File size:	595968 bytes
MD5 hash:	0E99D13AAFFCC5E8FADC45D8B85336D9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none">• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.689155208.000000000288A000.00000004.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.689464774.0000000003849000.00000004.00000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.689464774.0000000003849000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.689464774.0000000003849000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.689085196.0000000002841000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

[File Activities](#)

Show Windows behavior

- File Created
- File Written
- File Read

Analysis Process: Fp4grWelSC.exe PID: 6436 Parent PID: 7132

General

Start time:	20:22:32
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\Fp4grWelSC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Fp4grWelSC.exe
Imagebase:	0xab0000
File size:	595968 bytes
MD5 hash:	0E99D13AAFFCC5E8FADC45D8B85336D9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	<ul style="list-style-type: none">• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.686284909.0000000000400000.00000040.00000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.686284909.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.686284909.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.686745373.0000000000400000.00000040.00000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.686745373.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.686745373.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.764098779.0000000001080000.00000040.00020000.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.764098779.0000000001080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.764098779.0000000001080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.763833040.0000000000400000.00000040.00000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.763833040.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.763833040.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.764953786.0000000001820000.00000040.00020000.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.764953786.0000000001820000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.764953786.0000000001820000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

[File Activities](#)

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6436

General	
Start time:	20:22:35
Start date:	13/01/2022
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:	<ul style="list-style-type: none"> • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.719080265.000000000E88F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.719080265.000000000E88F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.719080265.000000000E88F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.740140108.000000000E88F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.740140108.000000000E88F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.740140108.000000000E88F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: autochk.exe PID: 6860 Parent PID: 3424

General

Start time:	20:23:06
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0x10c0000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 7036 Parent PID: 3424

General

Start time:	20:23:07
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.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

Yara matches:

- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.939516998.00000000007C0000.00000040.00020000.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.939516998.00000000007C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.939516998.00000000007C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.939085095.0000000000600000.00000040.00020000.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.939085095.0000000000600000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.939085095.0000000000600000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.941177470.0000000000BD0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.941177470.0000000000BD0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.941177470.0000000000BD0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Reputation: high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7080 Parent PID: 7036

General

Start time:	20:23:10
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Fp4grWeISC.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: 7020 Parent PID: 7080

General

Start time:	20:23:11
Start date:	13/01/2022
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

Analysis Process: explorer.exe PID: 5396 Parent PID: 5256

General

Start time:	20:23:42
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6fee60000
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

Registry Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 3460 Parent PID: 576

General

Start time:	20:24:17
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	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
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis