

JOESandbox Cloud BASIC



ID: 528718

Sample Name: STATEMENT

Oct-Nov 25-11-2021.com

Cookbook: default.jbs

Time: 17:48:31

Date: 25/11/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report STATEMENT Oct-Nov 25-11-2021.com	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
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:	7
Remote Access Functionality:	7
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	11
URLs	11
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	14
General	14
Entrypoint Preview	14
Rich Headers	14
Data Directories	14
Sections	14
Resources	14
Imports	14
Possible Origin	14
Network Behavior	14
Code Manipulations	14
Statistics	15
Behavior	15
System Behavior	15
Analysis Process: STATEMENT Oct-Nov 25-11-2021.exe PID: 6448 Parent PID: 2868	15
General	15
File Activities	15
File Created	15
File Deleted	15
File Written	15
File Read	15
Analysis Process: STATEMENT Oct-Nov 25-11-2021.exe PID: 6484 Parent PID: 6448	15
General	15

File Activities	16
File Read	16
Analysis Process: explorer.exe PID: 3292 Parent PID: 6484	16
General	16
Analysis Process: help.exe PID: 3516 Parent PID: 3292	17
General	17
File Activities	17
File Read	17
Analysis Process: cmd.exe PID: 5748 Parent PID: 3516	18
General	18
File Activities	18
Analysis Process: conhost.exe PID: 668 Parent PID: 5748	18
General	18
Analysis Process: explorer.exe PID: 7028 Parent PID: 8	18
General	18
File Activities	18
Registry Activities	18
Analysis Process: explorer.exe PID: 2268 Parent PID: 3512	19
General	19
File Activities	19
Registry Activities	19
Disassembly	19
Code Analysis	19

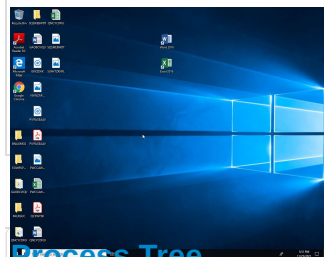
Windows Analysis Report STATEMENT Oct-Nov 25-11-2...

Overview

General Information

Sample Name:	STATEMENT Oct-Nov 25-11-2021.com (renamed file extension from com to exe)
Analysis ID:	528718
MD5:	02e738dd13974a..
SHA1:	6134aee9ceffce4..
SHA256:	9acf8fb51cab55a..
Tags:	exe Formbook
Infos:	

Most interesting Screenshots:



Process Tree

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

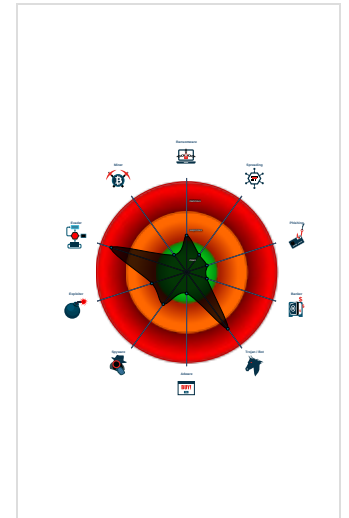
FormBook

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

Signatures

- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through ...)
- Multi AV Scanner detection for doma...
- Antivirus detection for dropped file
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an...
- Self deletion via cmd delete
- Injects a PE file into a foreign proce...
- Queues an APC in another process ...
- Tries to detect virtualization through...
- Machine Learning detection for dropp...

Classification



- System is w10x64
- STATEMENT Oct-Nov 25-11-2021.exe (PID: 6448 cmdline: "C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe" MD5: 02E738DD13974AB64A472F6AA2F065A8)
 - STATEMENT Oct-Nov 25-11-2021.exe (PID: 6484 cmdline: "C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe" MD5: 02E738DD13974AB64A472F6AA2F065A8)
 - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 - help.exe (PID: 3516 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
 - cmd.exe (PID: 5748 cmdline: /c del "C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - conhost.exe (PID: 668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - explorer.exe (PID: 7028 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 - explorer.exe (PID: 2268 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- cleanup

Malware Configuration

Threatname: FormBook

```

{
  "C2 list": [
    "www.davanamays.com/unzn/"
  ],
  "decoy": [
    "xiulf.com",
    "highcountrymortar.com",
    "523561.com",
    "marketingagency.tools",
    "gammovie.net",
    "nationaalcontactpunt.com",
    "sirrbter.com",
    "begizas.xyz",
    "missimi-fashion.com",
    "munixc.info",
    "daas.support",
    "spaceworbc.com",
    "faithtruthresolve.com",
    "gymkub.com",
    "thegrayverse.xyz",
    "artisanmakefurniture.com",
    "029tryy.com",
    "ijuubx.biz",
    "iphone13promax.club",
    "techuniversus.com",
    "samrgov.xyz",
    "growupcurl.com",
    "sj0755.net",
    "beekeeperkit.com",
    "richessesabondantes.com",
    "xclgjjh.net",
    "webworkscork.com",
    "vedepviet365.com",
    "bretabeaneven.com",
    "cdzsmhw.com",
    "clearperspective.biz",
    "tigr5g784sh.biz",
    "bbezan011.xyz",
    "mycar.store",
    "mansooralobeidli.com",
    "ascensionmemberszoom.com",
    "unlimitedrehab.com",
    "wozka.top",
    "askylarkgoods.com",
    "rj793.com",
    "prosvaor.com",
    "primetimeexpress.com",
    "boixosnoisperu.com",
    "mmasportgear.com",
    "concertirianian.net",
    "hyponymys.info",
    "maila.one",
    "yti0fyic.xyz",
    "shashiprayag.com",
    "speedpromotorsports.com",
    "westchestercountyjunkcars.com",
    "patienceinmypocket.com",
    "rausachbaoloc.com",
    "plexregroup.com",
    "outsyders.com",
    "foodandflour.com",
    "lenacrypto.xyz",
    "homeservicetoday.net",
    "marthaperry.com",
    "vmtcyd4q8.com",
    "shamefulguys.com",
    "locssol.store",
    "gnarledportra.xyz",
    "042atk.xyz"
  ]
}

```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.310494411.000000000400000.00000 040.00000001.sdmmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.310494411.0000000000400000.0000040.00000001.sdmp	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 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
00000002.00000002.310494411.0000000000400000.0000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> 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
00000002.00000001.257390266.0000000000400000.0000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000001.257390266.0000000000400000.0000040.00020000.sdmp	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 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

Click to see the 31 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.STATEMENT Oct-Nov 25-11-2021.exe.2940000.1.unpacked	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.STATEMENT Oct-Nov 25-11-2021.exe.2940000.1.unpacked	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 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
1.2.STATEMENT Oct-Nov 25-11-2021.exe.2940000.1.unpacked	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> 0x15cc9:\$sqlite3step: 68 34 1C 7B E1 0x15ddc:\$sqlite3step: 68 34 1C 7B E1 0x15cf8:\$sqlite3text: 68 38 2A 90 C5 0x15e1d:\$sqlite3text: 68 38 2A 90 C5 0x15d0b:\$sqlite3blob: 68 53 D8 7F 8C 0x15e33:\$sqlite3blob: 68 53 D8 7F 8C
2.1.STATEMENT Oct-Nov 25-11-2021.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.STATEMENT Oct-Nov 25-11-2021.exe.400000.0.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 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 28 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview



Click to jump to signature section

AV Detection:



Found malware configuration

Yara detected FormBook

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Machine Learning detection for dropped file

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected FormBook

System Summary:



Malicious sample detected (through community Yara rule)

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:



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

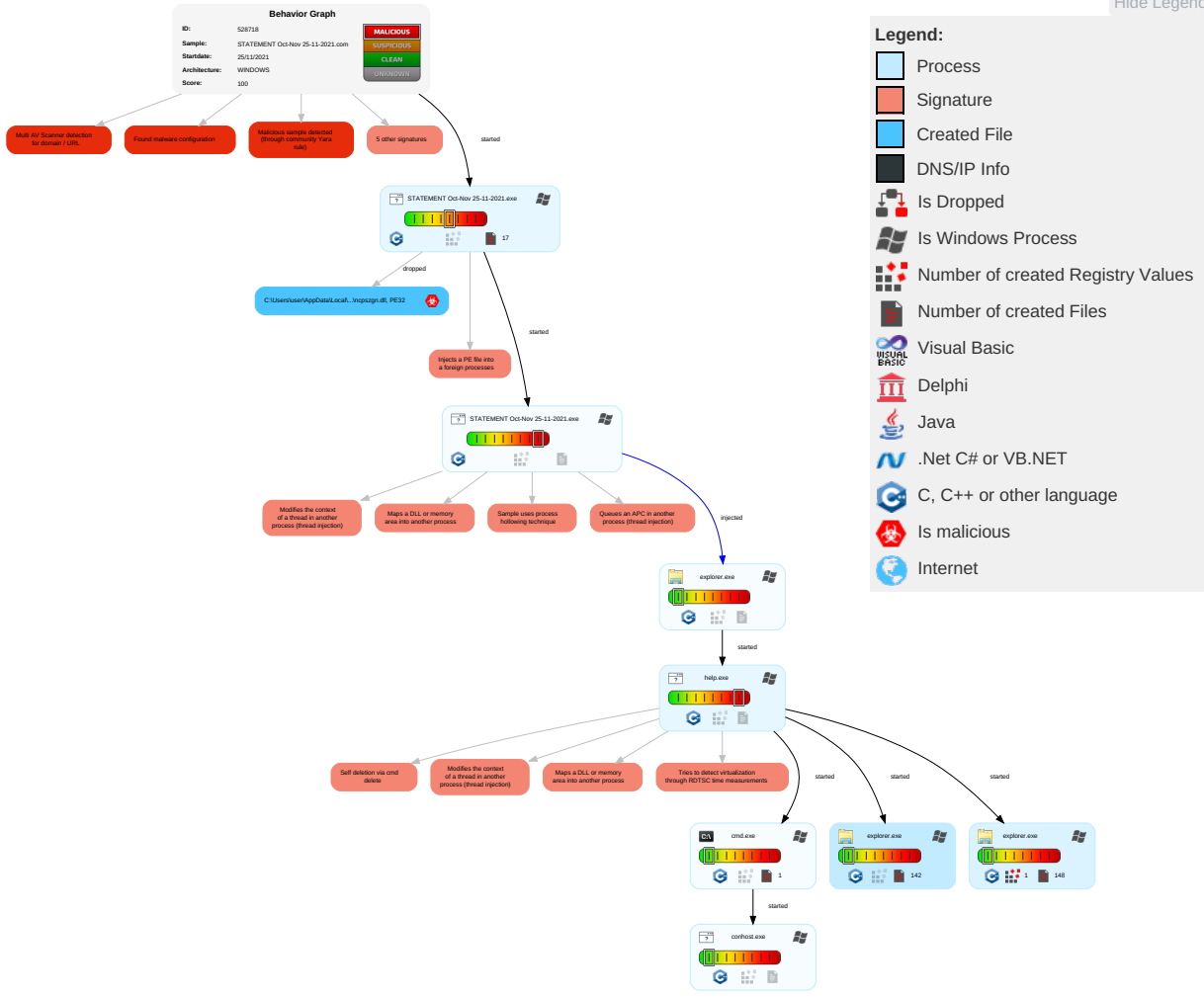
Remote Access Functionality:



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	Native API 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 7 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 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	Obfuscated Files or Information 3	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	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

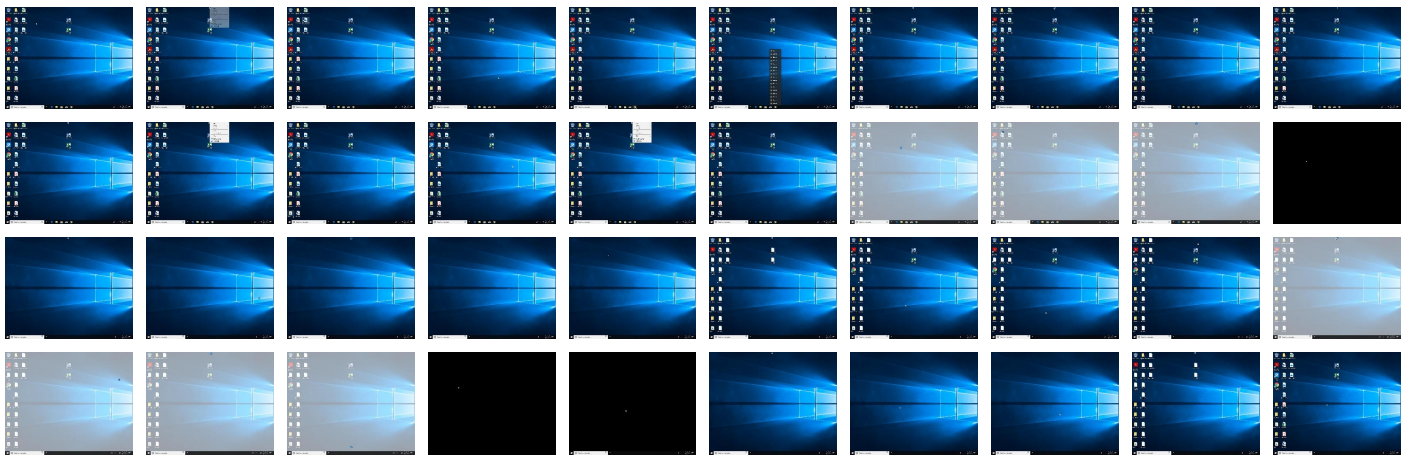
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsiE1DF.tmp\ncpszgn.dll	100%	Avira	HEUR/AGEN.1120891	
C:\Users\user\AppData\Local\Temp\nsiE1DF.tmp\ncpszgn.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.STATEMENT Oct-Nov 25-11-2021.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
2.1.STATEMENT Oct-Nov 25-11-2021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
23.0.explorer.exe.760796c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.STATEMENT Oct-Nov 25-11-2021.exe.2940000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.STATEMENT Oct-Nov 25-11-2021.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
23.0.explorer.exe.760796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.STATEMENT Oct-Nov 25-11-2021.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1120891		Download File
35.0.explorer.exe.82f796c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.help.exe.39a796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.help.exe.41d8a8.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
23.0.explorer.exe.760796c.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.STATEMENT Oct-Nov 25-11-2021.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.STATEMENT Oct-Nov 25-11-2021.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.STATEMENT Oct-Nov 25-11-2021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
35.2.explorer.exe.82f796c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.davanamays.com/unzn/	8%	Virustotal		Browse
www.davanamays.com/unzn/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.davanamays.com/unzn/	true	<ul style="list-style-type: none"> 8%, Virustotal, Browse Avira URL Cloud: safe 	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528718
Start date:	25.11.2021
Start time:	17:48:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	STATEMENT Oct-Nov 25-11-2021.com (renamed file extension from com to 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:	38
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@9/2@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> • Successful, ratio: 26.7% (good quality ratio 24.1%) • Quality average: 73.8% • Quality standard deviation: 32.2%
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> • Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:50:39	API Interceptor	149x 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\Templa66g5g72a86y4s 	
Process:	C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe
File Type:	data
Category:	dropped
Size (bytes):	217921
Entropy (8bit):	7.993006258714848
Encrypted:	true
SSDEEP:	3072:PFMHlejS23i+iJRw6Sq5C9O1qTNCY3ZR4YPaFnqAv8SGoFC8SwGDxB11y7N+EIY:PFslUJRWEEIsxCcR4xgQ3C87IBuk5
MD5:	1D70B490556922498B42E9CE56CB8D8A
SHA1:	884D47ED8FD75C8F68655D94DE2C2B3AA858A5D8
SHA-256:	F23DAAC89A555B61A44CBE1CFCD9373E2478E7B29AF8F97F176C91EED9084B76
SHA-512:	B2B811F1A727EF0D407EA8FC2317966444BE0B4FE87C274D2FD9D592CA8F8820B97FD383B7F1392EA4FA2C63207C3807E7B405EA3B2AACEDB971ABE799337E71


C:\Users\user\AppData\Local\Temp\66g5g72a86y4s	
Malicious:	false
Reputation:	low
Preview:	3...}...z...g.EH?rH...?^1%.n.....j.8:a?..... R.0...a.i.[c.".....U'....7.a.....+..t.Y...]{u.&...F.. \lz.dS.@s.l.#q.j{N.5}.t.T4..df.p...o.(E.oP...p...6j.B..g..... . .Ac...""7;.... .@a.k.@.....};5.....8.4.H.'; ..l.....}.....+...Ep1....<jW^1.n.....8:a?..... .R.?...a79>*"-.....Y..l5..h.....'F.....>.S"...mA.....F... .L.@4&A...?g...x.H.....e.d1P7&H\...{.P..B.3...X..... . .Ac.9.R.....m..@a.k.@_...9};.....{4.H.:> ..l.;...}.....w+...E.1....\j.^1%.n.....j.8:a?..... .R.?...a79>*"-.....Y..l5..h.....'F.....>.S"...mA.....F... . .L.@4&A...?g...x.H.....e.d1P7&H\.....6j.B...G...a... . .Ac.9.R.....m . @a.k.@_...9};.....{4.H.:> ..l.;...}.....w+...E.1....\j.^1%.n.....j.8:a?..... .R.?...a79>*"-.....Y..l5..h.....'F.....>.S"...mA.....F... . .L.@4&A...?g...x.H.....e.d1P7&H\.....6j.B...G...a... . .Ac.9.R.....m . @a.k.@_...9};

C:\Users\user\AppData\Local\Temp\InsiE1DF.tmp\ncpszgn.dll	
Process:	C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	89088
Entropy (8bit):	6.404549025482599
Encrypted:	false
SSDEEP:	1536:jrgK7figbwJzpTzjgANndassDD/7AQRmLXhtLbUfs2IExJ:jrf7igb69hZnLQOLxtL+x
MD5:	C3678C74295FF18273F177D3058BCC9D
SHA1:	619A2FBFB1F1512E96AF74733345E5539786E789
SHA-256:	D6CB2032B903D1820CC840659D655877CBA6D1E6746EBF366696AED3D9DC0C65
SHA-512:	3542B7DFEEA67460F52FD40F212831EBC33A7831B3B05770CE619C0E25F030129028E5E96C3291FC578D39075107E7EF8BF5883EA79A38C69A0EDEE9DF72056C
Malicious:	true
Antivirus:	<ul style="list-style-type: none"> Antivirus: Avira, Detection: 100% Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZx.....@.....x.....!..L!This program cannot be run in DOS mode.\$..PE..L.....a.....!.....v.....R..L...S...../..H.....U.....text.....`rdata...a.....b.....@..@.data...(.. .p.....H.....@...rsrc.....Z.....@..@...../..H.....U.....text.....@..@.data...(..

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.865250344327481
TrID:	<ul style="list-style-type: none"> Win32 Executable (generic) a (10002005/4) 92.16% NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% 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:	STATEMENT Oct-Nov 25-11-2021.exe
File size:	309066
MD5:	02e738dd13974ab64a472f6aa2f065a8
SHA1:	6134aee9ceffce4d6ed177739493def77b62533
SHA256:	9acf8fb51cab55a01a74cb84ca9958862b29b8909408e87412700e63a4f578ae
SHA512:	90ce5711d1f3abd07398c38706f5dc48da02676a8633115b5c7724fd98b1b41606f3d80763d3c03663c1c1bf7864609d65eae183b73f5df2db8e73a49bccf09
SSDEEP:	6144:jGiOxrmz8TDb8P0k87FSITkQ3nWFdYhBukErhH:6Fmz8TDbLkcolM742DsrhH
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.....uJ...\$... \$..\$/.{.\$...%.:\$. "y...\$..7...\$.f"...\$.Rich..\$.P E..L.....H.....\.....0.....

File Icon

	
Icon Hash:	0d32b232f3c8c453

Static PE Info

General

Entrypoint:	0x4030e3
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:	
Time Stamp:	0x48EFCDCD [Fri Oct 10 21:49:01 2008 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories


Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	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	0x4148	0x4200	False	0.218039772727	data	4.00493607489	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

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: STATEMENT Oct-Nov 25-11-2021.exe PID: 6448 Parent PID: 2868

General

Start time:	17:49:30
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe"
Imagebase:	0x400000
File size:	309066 bytes
MD5 hash:	02E738DD13974AB64A472F6AA2F065A8
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: 00000001.00000002.259654857.0000000002940000.00000004.00000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.259654857.0000000002940000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.259654857.0000000002940000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: STATEMENT Oct-Nov 25-11-2021.exe PID: 6484 Parent PID: 6448

General

Start time:	17:49:32
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe"
Imagebase:	0x400000
File size:	309066 bytes
MD5 hash:	02E738DD13974AB64A472F6AA2F065A8

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: 00000002.00000002.310494411.000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.310494411.000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.310494411.000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.257390266.000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.257390266.000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.257390266.000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.310637175.0000000005C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.310637175.0000000005C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.310637175.0000000005C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.310690464.0000000005F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.310690464.0000000005F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.310690464.0000000005F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.256870202.000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.256870202.000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.256870202.000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.256084055.000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.256084055.000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.256084055.000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 6484

General

Start time:	17:49:36
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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: 00000005.00000000.298278377.00000000EA41000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.298278377.00000000EA41000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.298278377.00000000EA41000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.285449444.00000000EA41000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.285449444.00000000EA41000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.285449444.00000000EA41000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: help.exe PID: 3516 Parent PID: 3292

General

Start time:	17:49:56
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x3a0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 0000000D.00000002.546085020.000000002F20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.546085020.000000002F20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.546085020.000000002F20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.546402750.0000000003220000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.546402750.0000000003220000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.546402750.0000000003220000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.545597108.000000000700000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.545597108.000000000700000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.545597108.000000000700000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5748 Parent PID: 3516**General**

Start time:	17:50:00
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\STATEMENT Oct-Nov 25-11-2021.exe"
Imagebase:	0x870000
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: 668 Parent PID: 5748**General**

Start time:	17:50:01
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 7028 Parent PID: 8**General**

Start time:	17:50:37
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff662bf0000
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: 2268 Parent PID: 3512

General

Start time:	17:51:16
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff662bf0000
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