



ID: 433069

Sample Name: bVsKNuwn30

Cookbook: default.jbs

Time: 08:49:25

Date: 11/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report bVsKNuwn30	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: FormBook	4
Yara Overview	5
Initial Sample	5
Dropped Files	5
Memory Dumps	6
Unpacked PEs	6
Sigma Overview	7
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:	7
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	11
URLs	11
Domains and IPs	12
Contacted Domains	12
Contacted URLs	12
URLs from Memory and Binaries	12
Contacted IPs	12
General Information	12
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASN	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	14
Static File Info	15
General	15
File Icon	15
Static PE Info	15
General	15
Authenticode Signature	15
Entrypoint Preview	16
Data Directories	16
Sections	16
Resources	16
Imports	16
Version Infos	16
Network Behavior	16
Code Manipulations	16
User Modules	16
Hook Summary	16
Processes	16
Statistics	16
Behavior	16
System Behavior	16
Analysis Process: bVsKNuwn30.exe PID: 6700 Parent PID: 6008	17
General	17

File Activities	17
File Created	17
File Written	17
File Read	17
Analysis Process: bVsKNuwn30.exe PID: 5612 Parent PID: 6700	17
General	17
File Activities	18
File Read	18
Analysis Process: explorer.exe PID: 3440 Parent PID: 5612	18
General	19
Analysis Process: msieexec.exe PID: 3532 Parent PID: 3440	19
General	19
File Activities	19
File Read	20
Analysis Process: cmd.exe PID: 5548 Parent PID: 3532	20
General	20
File Activities	20
Analysis Process: conhost.exe PID: 5560 Parent PID: 5548	20
General	20
Disassembly	20
Code Analysis	20

Analysis Report bVsKNuwn30

Overview

General Information

Sample Name:	bVsKNuwn30 (renamed file extension from none to exe)
Analysis ID:	433069
MD5:	3c88c6ef1a906bc..
SHA1:	1007ea59d9c209..
SHA256:	1754283e0b6bbb..
Tags:	exe trojan
Infos:	
Most interesting Screenshot:	

Detection



Score: 100

Range: 0 - 100

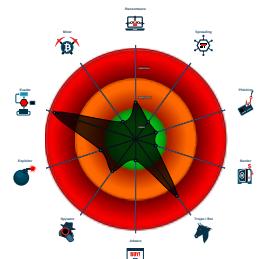
Whitelisted: false

Confidence: 100%

Signatures

- Found malware configuration
- Malicious sample detected (through ...)
- Multi AV Scanner detection for dropp...
- Multi AV Scanner detection for subm...
- Yara detected FormBook
- C2 URLs / IPs found in malware con...
- Machine Learning detection for dropp...
- Machine Learning detection for samp...
- Maps a DLL or memory area into an...
- Modifies the context of a thread in a...
- Modifies the prolog of user mode fun...
- Queues an APC in another process ...

Classification



Process Tree

- System is w10x64
- bVsKNuwn30.exe (PID: 6700 cmdline: 'C:\Users\user\Desktop\bVsKNuwn30.exe' MD5: 3C88C6EF1A906BC81FC6B5B7FC478E0C)
 - bVsKNuwn30.exe (PID: 5612 cmdline: C:\Users\user\AppData\Local\Temp\bVsKNuwn30.exe MD5: 3C88C6EF1A906BC81FC6B5B7FC478E0C)
 - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 - msieexec.exe (PID: 3532 cmdline: C:\Windows\SysWOW64\msieexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
 - cmd.exe (PID: 5548 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\bVsKNuwn30.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - conhost.exe (PID: 5560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cleanup

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bucksnortneola.com/gw2/"
  ],
  "decoy": [
    "knapc.com",
    "swagsoldier.com",
    "achochapo.com",
    "nestymentmaestra.com",
    "rakuen-beans.info",
    "portaldainsolencia.com",
    "nationaltodaytv.com",
    "monadiclab.com",
    "thebudgetfurnituredenver.com",
    "sifangzhouzi.com",
    "quangcaosonthach.com",
    "cbluebeltliveshop.com",
    "hyperrealmarketing.com",
    "dallasproducecompany.com",
    "zizhizhengshu.com",
    "becosyshe.com",
    "injectionhub.com",
    "wasteshelter.com",
    "gapegod.com",
    "danfrem.com",
    "emag.enterprises",
    "insomniaut.com",
    "margaretsboutiquenb.com",
    "bestmovies4k.com",
    "hsxytz.com",
    "veles.asia",
    "graphicoustic.com",
    "rzeroxi.com",
    "cristyleebennett.com",
    "vercoicsporno.club",
    "awdworldwide.com",
    "agrilast.com",
    "vineyardplaceseniorliving.com",
    "blancaholidaylets.com",
    "didixun.com",
    "localmiller.com",
    "gravityphysiotherapy.com",
    "couchtabledesktop.com",
    "cypresswoodsseniorliving.com",
    "mndastro.com",
    "opportunitybsi.com",
    "deejspeaks.com",
    "allivesmattertojesus.info",
    "clippingpathmask.com",
    "twoitrechuatraisudo.i.site",
    "mipcheritage.info",
    "acadeopolis.com",
    "52jnh.com",
    "thertrust.place",
    "highseachartersct.com",
    "booklarge.com",
    "kela-de.com",
    "ed-it-pantomath.com",
    "tricountyrr.com",
    "blackeye.online",
    "hidrovaco.com",
    "sleeplessreconnaissance.life",
    "newalbanyironworks.com",
    "scthx.b.com",
    "bosssss.com",
    "isaostar.com",
    "pointredeem.com",
    "myfulfillmentproject.com",
    "toikawai.com"
  ]
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
bVsKNuwn30.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\bVsKNuhn30.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.598613776.0000000000D2 0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.598613776.0000000000D2 0000.00000004.00000001.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"> • 0x98e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xb62:\$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 • 0xb327:\$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xc32a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000013.00000002.598613776.0000000000D2 0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> • 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
00000013.00000002.598554261.0000000000CF 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.598554261.0000000000CF 0000.00000040.00000001.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"> • 0x98e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xb62:\$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 • 0xb327:\$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xc32a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 36 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.bVsKNuhn30.exe.660000.1.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
19.2.msiexec.exe.4eef834.4.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0.2.bVsKNuhn30.exe.6f0000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
12.2.bVsKNuhn30.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.2.bVsKNuhn30.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"> • 0x8ae8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xb62:\$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 17 entries

Sigma Overview

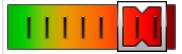
No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

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:



Yara detected Costura Assembly Loader

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



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:



Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:



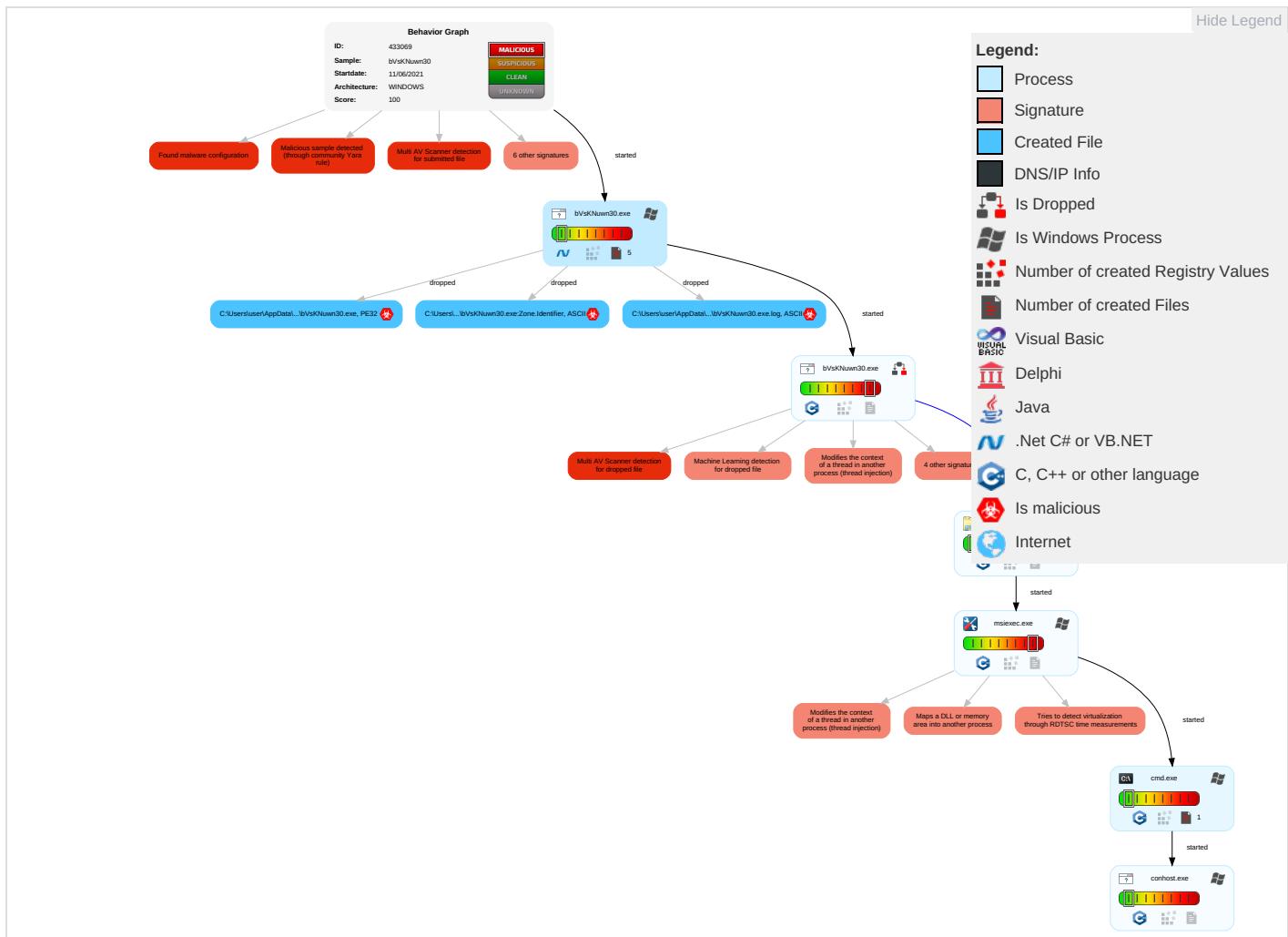


Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	Process Injection 4 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	System Information Discovery 1 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 4 1 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	DLL Side-Loading 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

Behavior Graph

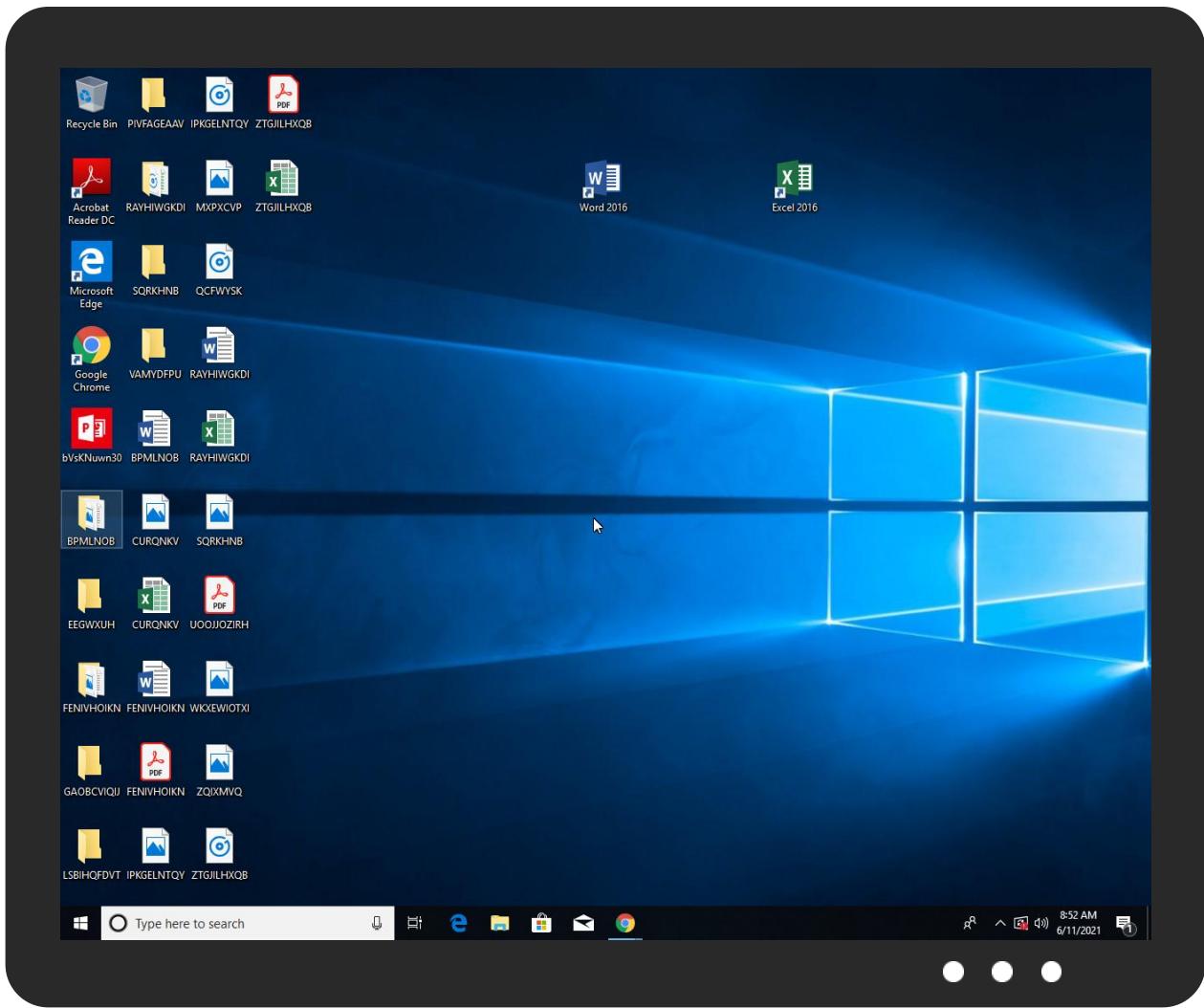


Screenshots

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
bVsKNuhn30.exe	51%	Virustotal		Browse
bVsKNuhn30.exe	26%	Metadefender		Browse
bVsKNuhn30.exe	55%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
bVsKNuhn30.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\bVsKNuhn30.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bVsKNuhn30.exe	51%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\bVsKNuhn30.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\bVsKNuhn30.exe	55%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.bVsKNuhn30.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.bVsKNuhn30.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://sectigo.com/CPSOU	0%	URL Reputation	safe	
http://https://sectigo.com/CPSOU	0%	URL Reputation	safe	
http://https://sectigo.com/CPSOU	0%	URL Reputation	safe	
http://https://sectigo.com/CPSOU	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
www.bucksnortheola.com/gw2/	1%	Virustotal		Browse
www.bucksnortheola.com/gw2/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://sectigo.com/CPSOD	0%	URL Reputation	safe	
http://https://sectigo.com/CPSOD	0%	URL Reputation	safe	
http://https://sectigo.com/CPSOD	0%	URL Reputation	safe	
http://https://sectigo.com/CPSOD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.bucksnortheola.com/gw2/	true	<ul style="list-style-type: none"> 1%, Virustotal, Browse Avira URL Cloud: safe 	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433069
Start date:	11.06.2021
Start time:	08:49:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 27s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	bVsKNUwn30 (renamed file extension from none 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:	24
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@7/3@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> • Successful, ratio: 15.5% (good quality ratio 13.9%) • Quality average: 74.7% • Quality standard deviation: 31.3%
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 96% • 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

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\lbVsKNUwn30.exe	RFL_PO_69002.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VsKNuwn30.exe.log	
Process:	C:\Users\user\Desktop\lbVsKNuwn30.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDeep:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJkiUrRZ9l0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADDD
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eeafa3cd3e0ba98b5ebdbbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\bVsKNuwn30.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\bVsKNuwn30.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	true
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.949126101574067
TrID:	<ul style="list-style-type: none"> Win32 Executable (generic) Net Framework (10011505/4) 50.01% Win32 Executable (generic) a (10002005/4) 49.97% Generic Win/DOS Executable (2004/3) 0.01% DOS Executable Generic (2002/1) 0.01% Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	bVsKNuwn30.exe
File size:	533488
MD5:	3c88c6ef1a906bc81fc6b5b7fc478e0c
SHA1:	1007ea59d9c209f367a1873ae6da2eac5fad81ef
SHA256:	1754283e0b6bbbbe69f165e54e3795d3e34ca14aa7bd8bd3b7dcdd97f7dfca8
SHA512:	87841b94db9f67d856cbcc4e14be6ab56716ffca161adcf23ea5931ed3a2843c5207004e0e5ae7e9e764d9d28259c3e2565be10600134b89677f7734457a0f0
SSDEEP:	12288:A4tWKG1Gu7iTQezjBwaxITEI3ENCYyuqoTGYA6TJqiU1:A4tc1Gu7Kzurgl3FBOAmqb1
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$.....PE...L...^ .i.....0.....J.....@.....@.....@.....@.....

File Icon



Icon Hash:

23d8dcd2d8d85047

Static PE Info

General

Entrypoint:	0x47cfde
Entrypoint Section:	.text
Digitally signed:	true
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:	0xD669075E [Tue Dec 28 08:16:30 2083 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

Authenticode Signature

Signature Valid:	false
Signature Issuer:	CN=COMODO RSA Extended Validation Code Signing CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	The digital signature of the object did not verify
Error Number:	-2146869232
Not Before, Not After	<ul style="list-style-type: none"> 10/6/2019 5:00:00 PM 10/6/2022 4:59:59 PM
Subject Chain	<ul style="list-style-type: none"> CN=Telegram FZ-LLC, O=Telegram FZ-LLC, STREET="Business Central Towers, Tower A, Office 2301 2303", L=Dubai, S=Dubai, C=AE, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=AE, SERIALNUMBER=94349

Version:	3
Thumbprint MD5:	034F2391B5CE85A7D99BC43FE240F70F
Thumbprint SHA-1:	D4C89B25D3E92D05B44BC32C0CBFD7693613F3EE
Thumbprint SHA-256:	E31F1B9C3DD0EDEFDF96F85B8FFD1DB976573BB262CC6E1154AD8FDC4D55449
Serial:	1F3216F428F850BE2C66CAA056F6D821

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7afe4	0x7b000	False	0.988739758003	data	7.99300765862	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x46e8	0x4800	False	0.0667860243056	data	2.5375520699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x84000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: bVsKNuhn30.exe PID: 6700 Parent PID: 6008

General

Start time:	08:50:21
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\bVsKNuhn30.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\bVsKNuhn30.exe'
Imagebase:	0x6f0000
File size:	533488 bytes
MD5 hash:	3C88C6EF1A906BC81FC6B5B7FC478E0C
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_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.489441014.000000003B96000.0000004.0000001.sdmp, Author: Joe SecurityRule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.489441014.000000003B96000.0000004.0000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot comRule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.489441014.000000003B96000.0000004.0000001.sdmp, Author: JPCERT/CC Incident Response GroupRule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.481505916.000000000CB7000.0000004.0000001.sdmp, Author: Joe SecurityRule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.486485678.000000002A41000.0000004.0000001.sdmp, Author: Joe SecurityRule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000000.331883063.0000000006F2000.0000002.00020000.sdmp, Author: Joe SecurityRule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.484632271.0000000006F2000.0000002.00020000.sdmp, Author: Joe SecurityRule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.489573896.0000000003C6A000.0000004.0000001.sdmp, Author: Joe SecurityRule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.489573896.0000000003C6A000.0000004.0000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot comRule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.489573896.0000000003C6A000.0000004.0000001.sdmp, Author: JPCERT/CC Incident Response GroupRule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.489676903.0000000003D04000.0000004.0000001.sdmp, Author: Joe SecurityRule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.489676903.0000000003D04000.0000004.0000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot comRule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.489676903.0000000003D04000.0000004.0000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: bVsKNuhn30.exe PID: 5612 Parent PID: 6700

General

Start time:	08:51:31
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\bVsKnuwn30.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\bVsKnuwn30.exe
Imagebase:	0x7ff7ae910000
File size:	533488 bytes
MD5 hash:	3C88C6EF1A906BC81FC6B5B7FC478E0C
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_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000C.00000000.482709799.0000000000662000.0000002.00020000.sdmp, Author: Joe Security Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000C.00000000.484079723.0000000000662000.0000002.00020000.sdmp, Author: Joe Security Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.484041587.000000000400000.0000040.00000001.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.484041587.000000000400000.0000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.484041587.000000000400000.0000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.542191970.0000000000C50000.0000040.00000001.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.542191970.0000000000C50000.0000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.542191970.0000000000C50000.0000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.542282401.0000000000DD0000.0000040.00000001.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.542282401.0000000000DD0000.0000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.542282401.0000000000DD0000.0000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000C.00000002.539491426.0000000000662000.0000002.00020000.sdmp, Author: Joe Security Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.538565739.0000000000400000.0000040.00000001.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.538565739.0000000000400000.0000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.538565739.0000000000400000.0000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\bVsKnuwn30.exe, Author: Joe Security
Antivirus matches:	<ul style="list-style-type: none"> Detection: 100%, Joe Sandbox ML Detection: 51%, Virustotal, Browse Detection: 26%, Metadefender, Browse Detection: 55%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 5612

General

Start time:	08:51:34
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msieexec.exe PID: 3532 Parent PID: 3440

General

Start time:	08:51:54
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\msieexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msieexec.exe
Imagebase:	0x10d0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
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: 00000013.00000002.598613776.0000000000D20000.0000004.0000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.598613776.0000000000D20000.0000004.0000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.598613776.0000000000D20000.0000004.0000001.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.598554261.0000000000CF0000.00000040.00000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.598554261.0000000000CF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.598554261.0000000000CF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000013.00000002.601052355.0000000004EEF000.0000004.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.598077257.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.598077257.00000000007B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.598077257.00000000007B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000013.00000002.599515980.000000000469F000.0000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5548 Parent PID: 3532

General

Start time:	08:52:00
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\bVsKNuhn30.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3DBDE3BB6F734E357235F4D5898582D
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: 5560 Parent PID: 5548

General

Start time:	08:52:00
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis