ID: 510423
Sample Name:
VJaX7U6LAp.exe
Cookbook: default.jbs
Time: 19:32:36
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

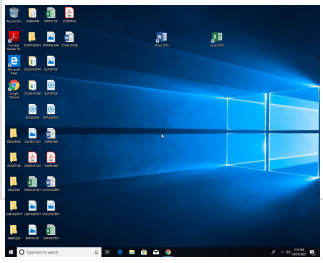
Windows Analysis Report VJaX7U6LAp.exe

Overview

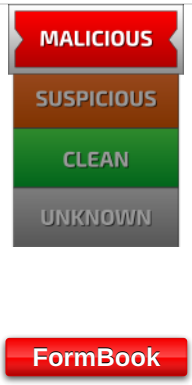
General Information

Sample Name:	VJaX7U6LAp.exe
Analysis ID:	510423
MD5:	15a4b8c6607b8e..
SHA1:	c77c0417b07c25...
SHA256:	c4b1789371d832..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



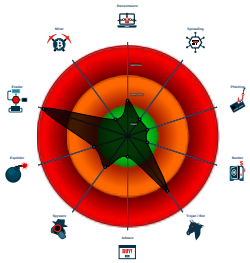
FormBook

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
- System process connects to networ...
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an...
- Tries to detect sandboxes and other...
- Modifies the prolog of user mode fun...
- Self deletion via cmd delete
- .NET source code contains potentia...

Classification



Process Tree

- **System is w10x64**
- VJaX7U6LAp.exe (PID: 6316 cmdline: 'C:\Users\user\Desktop\VJaX7U6LAp.exe' MD5: 15A4B8C6607B8E67B0BBA2D1B5DBD43E)
  - VJaX7U6LAp.exe (PID: 5088 cmdline: C:\Users\user\Desktop\VJaX7U6LAp.exe MD5: 15A4B8C6607B8E67B0BBA2D1B5DBD43E)
  - VJaX7U6LAp.exe (PID: 6284 cmdline: C:\Users\user\Desktop\VJaX7U6LAp.exe MD5: 15A4B8C6607B8E67B0BBA2D1B5DBD43E)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - help.exe (PID: 5040 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
        - cmd.exe (PID: 6932 cmdline: /c del 'C:\Users\user\Desktop\VJaX7U6LAp.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.zahnimplantatangebotede.com/mxwf/"
  ],
  "decoy": [
    "orders-cialis.info",
    "auctionorbuy.com",
    "meanmugsamore.com",
    "yachtcrewmark.com",
    "sacredkashilifestudio.net",
    "themintyard.com",
    "bragafoods.com",
    "sierp.com",
    "hausofdeme.com",
    "anthonyjames915.com",
    "bajardepesoencasa.com",
    "marciaroyal.com",
    "earringlifter.com",
    "dsdjfhd9ddksa1as.info",
    "bmzproekt.com",
    "employmentbc.com",
    "ptsdtreatment.space",
    "vrchance.com",
    "cnrongding.com",
    "welovelit.com",
    "intercourierdelivery.services",
    "ianwhitewrite.com",
    "afcerd.com",
    "beneficiodemedicare.com",
    "gatel3ess.com",
    "salesnksportswt.top",
    "thewellnessloft365.com",
    "totensa.com",
    "jessicatheisen.com",
    "snowtographers.com",
    "executrainpr.com",
    "puttypaw.com",
    "popcorntimeipad.com",
    "heyconi.com",
    "llanoresources.com",
    "ibusinesshero.com",
    "1euro1ad.com",
    "sparkleeapp.com",
    "zhuxiugyh.com",
    "calvinmaphoto.com",
    "bjmaomao.com",
    "isaacfujiki.com",
    "zipwhipper.com",
    "kontrollstutzen.com",
    "hannaheason.media",
    "zgcbw.net",
    "letteringdagabi.com",
    "kitefabrics.com",
    "andherieastoffices.com",
    "thewellnesstravelcompany.info",
    "ohio.works",
    "beacharita.com",
    "alphamillls.com",
    "sassandvinegar.com",
    "usauber.com",
    "ceylonherbslk.com",
    "richardggreenhill.com",
    "groupdae.com",
    "jupiterccc.com",
    "indoovo.com",
    "sunnytheodora.com",
    "gxpgfz.com",
    "shoppandaxpress.com",
    "heiboard.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.359814087.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.359814087.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000000.359814087.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000000.359438927.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000000.359438927.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.VJaX7U6LAp.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.VJaX7U6LAp.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.0.VJaX7U6LAp.exe.400000.6.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
4.0.VJaX7U6LAp.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.VJaX7U6LAp.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 23 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

Networking:

System process connects to network (likely due to code injection or exploit)

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:

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

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:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

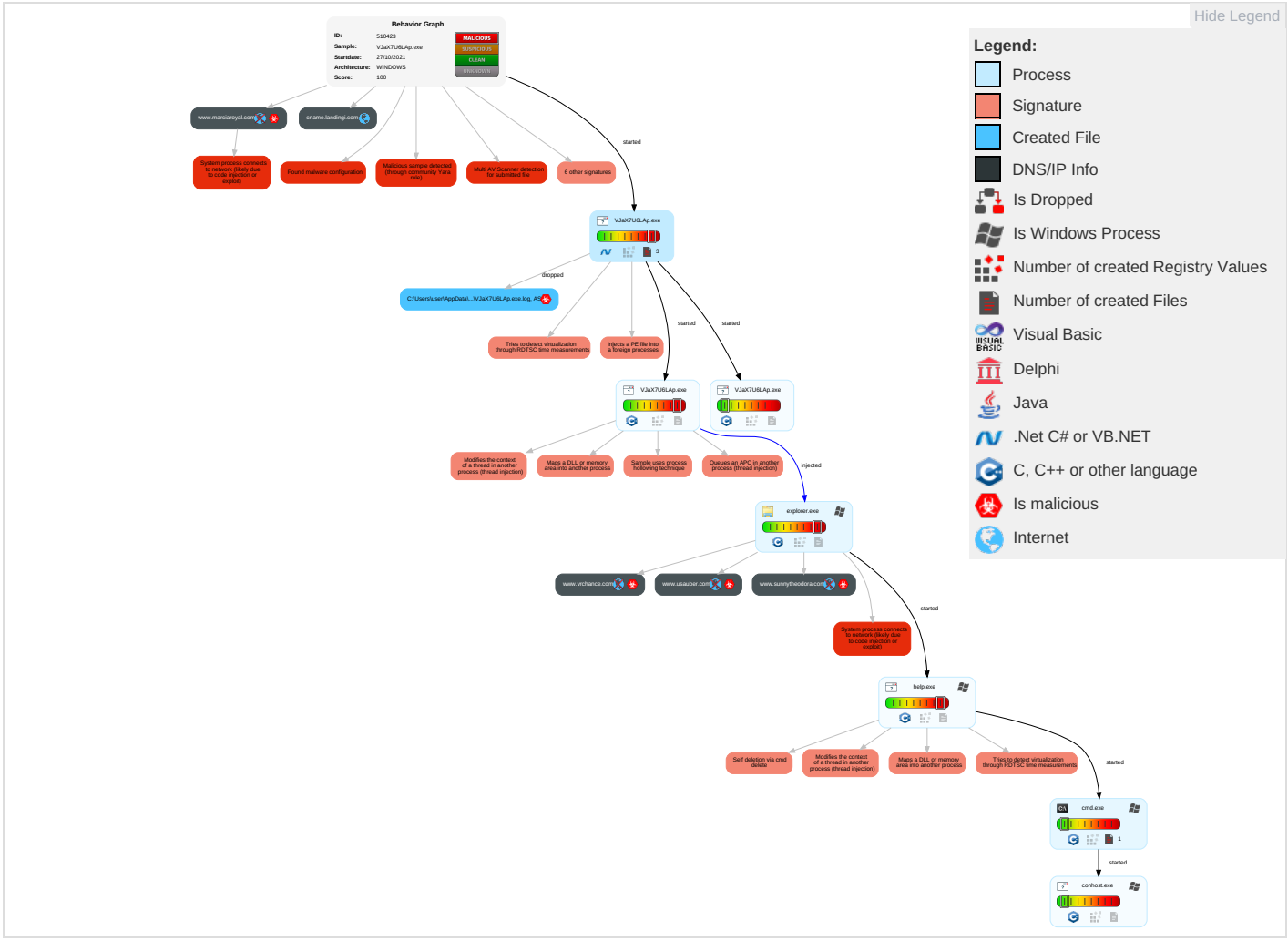
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
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	Application Layer Protocol 1 1	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
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	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	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 Cellu Base Statio

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
VJaX7U6LAp.exe	10%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.VJaX7U6LAp.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.VJaX7U6LAp.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.VJaX7U6LAp.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.VJaX7U6LAp.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
www.zahnimplantatangebotede.com/mxwf/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cname.landingi.com	54.77.19.84	true	false		high
www.usauber.com	unknown	unknown	true		unknown
www.marciaroyal.com	unknown	unknown	true		unknown
www.vrchance.com	unknown	unknown	true		unknown
www.sunnytheodora.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.zahnimplantatangebotede.com/mxwf/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510423
Start date:	27.10.2021
Start time:	19:32:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VJaX7U6LAp.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:	25
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/1@4/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.9% (good quality ratio 31.7%) • Quality average: 72.1% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:33:37	API Interceptor	1x Sleep call for process: VJaX7U6LAp.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cname.landingi.com	SDL_Order Onay#U0131 _ Acil,pdf.exe	Get hash	malicious	Browse	• 54.77.19.84
	DF_Nueva orden _WJO-001,pdf.exe	Get hash	malicious	Browse	• 108.128.238.226
	Yeni Sipari#U015f #86-55113,pdf.exe	Get hash	malicious	Browse	• 52.212.68.12
	ny5QHKcgLH.exe	Get hash	malicious	Browse	• 108.128.238.226
	IMG16092021.exe	Get hash	malicious	Browse	• 52.212.68.12
	ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 52.212.68.12
	0OBKA8AwTn.exe	Get hash	malicious	Browse	• 54.77.19.84
	ZbpMqzUXVN.exe	Get hash	malicious	Browse	• 108.128.238.226
	PO_IMG_13072021_item.exe	Get hash	malicious	Browse	• 52.212.68.12
	47mAsp9IER.exe	Get hash	malicious	Browse	• 54.77.19.84
	U03c2doc.exe	Get hash	malicious	Browse	• 108.128.238.226
	scan-copy059950059pdf.exe	Get hash	malicious	Browse	• 108.128.238.226
	SKMBT_C224307532DL23457845_Product Order doc.exe	Get hash	malicious	Browse	• 108.128.238.226
	Descripciones de oferta de productos MACIILIAS SRL doc.exe	Get hash	malicious	Browse	• 54.77.19.84
	a449cc12_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.212.68.12
	Dokument Nota odbiorcza IMI FFPT-2019223912003_2021 doc.exe	Get hash	malicious	Browse	• 108.128.238.226
	Documento de transfer#U00eancia banc#U00e1ria _2021doc.exe	Get hash	malicious	Browse	• 52.212.68.12
	TSVINCCU21021642.exe	Get hash	malicious	Browse	• 52.212.68.12
	SWIFT COPY.exe	Get hash	malicious	Browse	• 54.77.19.84
	SWIFT COPY.exe	Get hash	malicious	Browse	• 54.77.19.84

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\VJaX7U6LAp.exe.log	
Process:	C:\Users\user\Desktop\VJaX7U6LAp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.687486048595242
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	VJaX7U6LAp.exe
File size:	520192
MD5:	15a4b8c6607b8e67b0bba2d1b5dbd43e
SHA1:	c77c0417b07c25c0e567f0d0362a8a80fc7c40e9
SHA256:	c4b1789371d832969f812bd0a577e380cdac00db6775d7c251adf8d92c15d74
SHA512:	b168504f30e0714a8d2ec0eb79a9d49b5c1f84399ac0ee091fe9b4983e9ed77b9fd70398a6c2644b3295f777d3d9b84422f76897e722df579a1ef1dd66d8704c
SSDEEP:	12288:IaNilVYYYGC3tsZ1isByVk2t0iWbtY36yhPhQ:bNilBYui7m2t0iWY6yh
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..._.ya.....0.....J.... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48054a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6179805F [Wed Oct 27 16:37:51 2021 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	0x7e550	0x7e600	False	0.685342096316	data	6.69788098244	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x5c4	0x600	False	0.430989583333	data	4.15472453477	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x84000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 19:34:47.814812899 CEST	192.168.2.6	8.8.8.8	0xef69	Standard query (0)	www.usauber.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:35:04.025022030 CEST	192.168.2.6	8.8.8.8	0xdedd	Standard query (0)	www.sunnytheodora.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:35:24.880810976 CEST	192.168.2.6	8.8.8.8	0xc2a6	Standard query (0)	www.vrchance.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:35:47.099709988 CEST	192.168.2.6	8.8.8.8	0x4c2	Standard query (0)	www.marciaroyal.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 19:34:47.836822033 CEST	8.8.8.8	192.168.2.6	0xef69	Name error (3)	www.usauber.com	none	none	A (IP address)	IN (0x0001)
Oct 27, 2021 19:35:04.055140972 CEST	8.8.8.8	192.168.2.6	0xdedd	Name error (3)	www.sunnytheodora.com	none	none	A (IP address)	IN (0x0001)
Oct 27, 2021 19:35:47.126094103 CEST	8.8.8.8	192.168.2.6	0x4c2	No error (0)	www.marciaroyal.com	cname.landingi.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 19:35:47.126094103 CEST	8.8.8.8	192.168.2.6	0x4c2	No error (0)	cname.landingi.com		54.77.19.84	A (IP address)	IN (0x0001)
Oct 27, 2021 19:35:47.126094103 CEST	8.8.8.8	192.168.2.6	0x4c2	No error (0)	cname.landingi.com		52.212.68.12	A (IP address)	IN (0x0001)
Oct 27, 2021 19:35:47.126094103 CEST	8.8.8.8	192.168.2.6	0x4c2	No error (0)	cname.landingi.com		108.128.238.226	A (IP address)	IN (0x0001)

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: VJaX7U6LAp.exe PID: 6316 Parent PID: 5372

General

Start time:	19:33:36
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\VJaX7U6LAp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\VJaX7U6LAp.exe'
Imagebase:	0x140000
File size:	520192 bytes
MD5 hash:	15A4B8C6607B8E67B0BBA2D1B5DBD43E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.362891212.0000000003659000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.362891212.0000000003659000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.362891212.0000000003659000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.362570337.0000000002651000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: VJaX7U6LAp.exe PID: 5088 Parent PID: 6316

General

Start time:	19:33:38
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\VJaX7U6LAp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\VJaX7U6LAp.exe
Imagebase:	0x220000
File size:	520192 bytes
MD5 hash:	15A4B8C6607B8E67B0BBA2D1B5DBD43E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: VJaX7U6LAp.exe PID: 6284 Parent PID: 6316

General

Start time:	19:33:39
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\VJaX7U6LAp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\VJaX7U6LAp.exe
Imagebase:	0xb40000
File size:	520192 bytes
MD5 hash:	15A4B8C6607B8E67B0BBA2D1B5DBD43E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.359814087.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.359814087.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.359814087.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.359438927.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.359438927.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.359438927.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.428718419.00000000018A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.428718419.00000000018A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.428718419.00000000018A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.428663450.0000000001870000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.428663450.0000000001870000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.428663450.0000000001870000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.424469063.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.424469063.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.424469063.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6284

General

Start time:	19:33:42
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.392844589.000000000763B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.392844589.000000000763B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.392844589.000000000763B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.407150774.000000000763B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.407150774.000000000763B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.407150774.000000000763B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: help.exe PID: 5040 Parent PID: 3440

General

Start time:	19:34:06
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0xac0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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.00000002.620322575.0000000000990000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.620322575.0000000000990000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.620322575.0000000000990000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.620433344.00000000009C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.620433344.00000000009C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.620433344.00000000009C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.619605094.0000000000480000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.619605094.0000000000480000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.619605094.0000000000480000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6932 Parent PID: 5040

General

Start time:	19:34:12
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\VJaX7U6LAp.exe'
Imagebase:	0x2a0000
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: 6244 Parent PID: 6932

General

Start time:	19:34:14
Start date:	27/10/2021
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