

Tracking the World's Dumbest Cyber-Mercenaries

How to fail and still succeed



Respublika (Kazakh newspaper)

7 languages

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

Respublika (Russian: Республика – деловое оброзение) or ***Golos Respubliki*** (Voice of the Republic) was a weekly Russian-language Kazakhstani newspaper. Founded by Irina Petrushova in 2000, the paper is known for its reporting on government corruption. It was ordered to closure in 2002 and in May 2005 by the Ministry of Culture, Information and Sports,[1] but continued to publish under a variety of titles.[2] In late 2012, before the anniversary of the Mangystau riots, Kazakhstani authorities raided and searched *Respublika*'s office and again suspended its publication, pending a verdict on criminal charges.[3][4]

Respublika

Type	weekly
Founder(s)	Irina Petrushova
Founded	2000
Language	Russian
Ceased publication	2012
Headquarters	Almaty
Website	http://www.respublika-kaz.biz/

History [edit]

Russian journalist Irina Petrushova founded *Respublika* in 2000. The weekly focused on covering business and economic issues in Kazakhstan, and frequently published stories highly critical of Nazarbayev's regime. The paper wrote about financial scandals and rampant nepotism and cronyism. Scandals the paper exposed included the granting of oil rights to one of Nazarbayev's relatives; the disappearance of funds for an airport in the capital, Almaty; and the Kazakhstani police forcing tourists off a plane so that Nazarbayev's daughter might fly alone.[5][6] *Respublika*'s most notable story was an exposé which revealed that Nazarbayev had stashed US$1 billion of the state's oil revenues in a Swiss bank account; the government stated that this had been an emergency fund used to rescue the national economy in 1998.[5]

In November 2001, a government representative unsuccessfully attempted to buy a controlling stake in *Respublika*. In January 2002, Kazakhstani printers began to refuse to print the paper, one after a human skull was placed on his doorstep.[5]







KAZAWORD

Kaz news

Home About

О нас снова пишут...

May 6, 2016

http://www.zaprava.ru/201605055852/glavnyie-novosti-dnya/ne-dopusimi-ekstradicziyu-muxtara-ablyazova-iz-franczii-v-rossiyu

Открытое обращение российских правозащитников к представителям французских и британских властей, ООН, ЕС, ОБСЕ, и ПАСЕ, составленное на основании опубликованных в этом блоге документов. Обращение подписано Алексеевой Л.М., Борщевым В.В., Ганнушкиной С.А., Ковалевым С.А., Пономаревым Л.А., Световой З.Ф.

Leave a comment

Search ...

RECENT POSTS

О нас снова пишут...
Два товарища
Наращиваем темп публикаций
О работе наших коллег
С днем дурака!

RECENT COMMENTS

ARCHIVES

May 2016
April 2016
March 2016
April 2015
March 2015
February 2015

Gmail by Google

111 111 <nicprivat4@gmail.com>

Invoice Lexial ATABAYEV

1 письмо

eruc@lexial.eu <eruc@lexial.eu> 12 августа 2015 г., 13:06
Кому: lotus@bp-pb.com

Dear Bota,

As agreed, please find attached our invoice.

Thank you in advance for the payment.

Best regards,

E. Ruchat

LEXIAL
SOCIETE D'AVOCATS

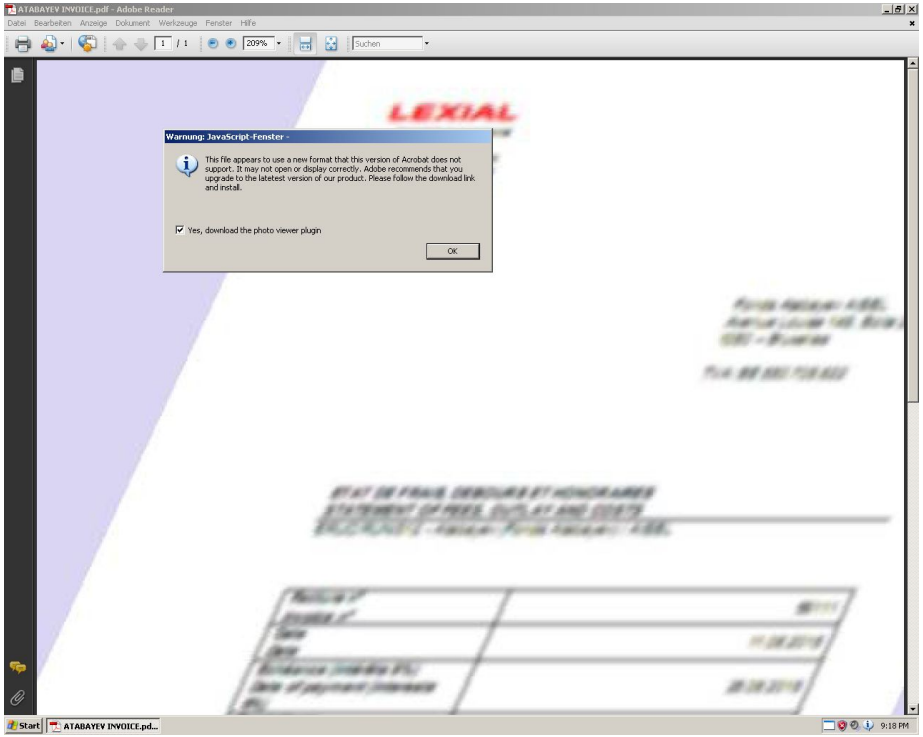
Brussels office : chaussée de Louvain 467, B-1030 Bruxelles - Tél. (English) (32)(0)2 880 79 52 – Tél. : (French) (32)(0)2 732 53 61 - Fax (32)(0)2 706 54 18

Paris office : 2 bis rue Guénégaud, F-75006 Paris - Tél. (33)(0)1 42 60 04 31 - Fax (33)(0)1 77 74 62 69

Geneva office: Route de St-Julien 184A, 1228 Plan-les-Ouates (Genève), Tel. : (41)(0) 951 08 25 - Fax : (41)(0) 22 594 80 88

This e-mail is sent from Lexial law firm. The content of this email and any attachments are confidential to the intended recipient. They may not be disclosed to or used by or copied in any way by anyone other than the intended recipient. If this e-mail is received in error, please contact us quoting the name of the sender and the email address to which it has been sent and then delete it.

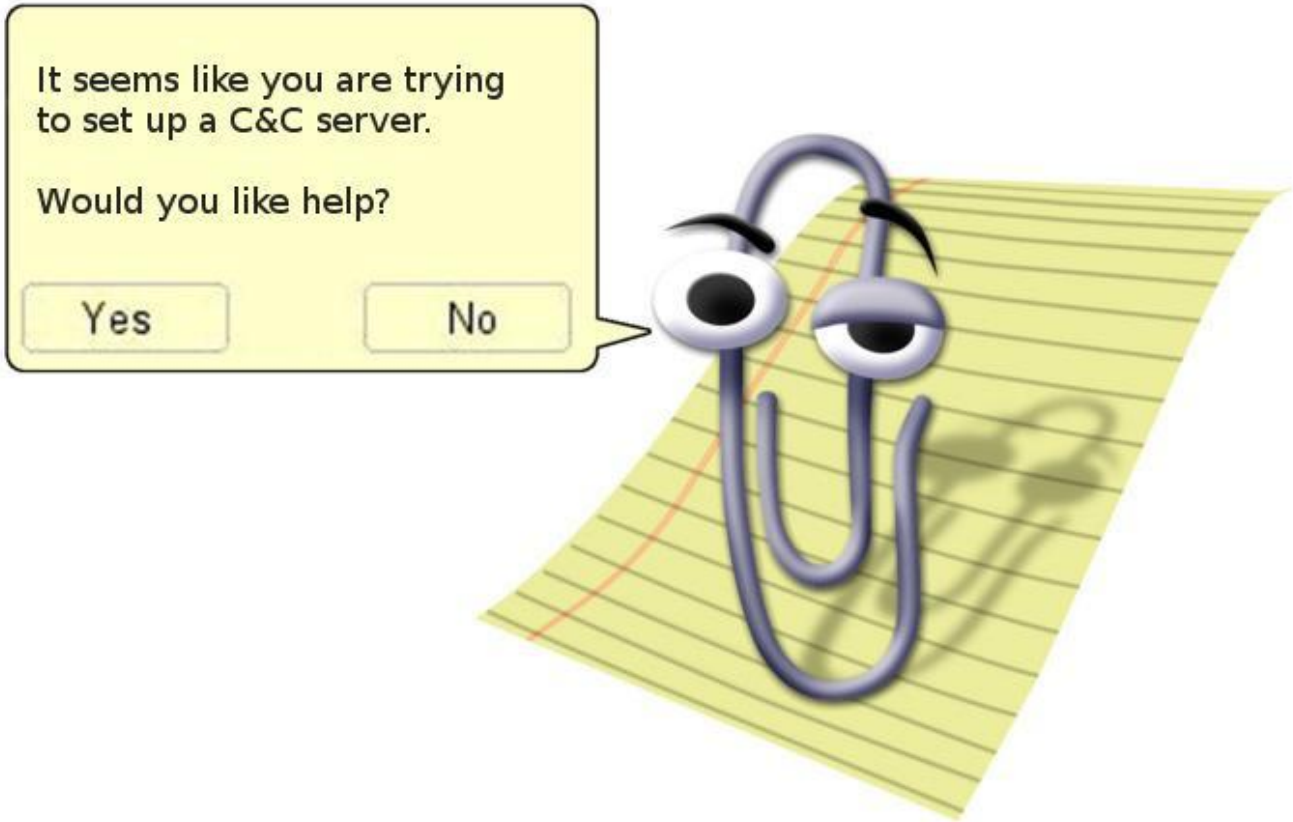
ATABAYEV INVOICE.pdf
31K




OPERATION
MANUL

Bandook Malware

CaptureScreen	DeleteFileFromDevice	DeleteAutoFTPFromDB	CompressArchive	StealUSB
Init	CopyMTP	ExecuteTV	GenerateReports	StartFileMonitor
ClearCred	ChromeInject	ExecuteAMMY	GetWifi	SendFileMonLog
GetCamlist	DisableChrome	DDOSON	StartShell	GetUSBMONLIST
SendCam	RarFolder	ExecuteTVNew	GetSound	GetFileMONLIST
StopCam	SendUSBList	getkey	SplitMyFile	StopUSBMonitor
Uninstall	SignoutSkype	SendMTPList	GetAutoFTP	SearchMain
SendStartup	StopSearch	SendMTPList2	GrabFileFromDevice	PutFileOnDevice
StopFileMonitor	SendinfoList	EnableAndLoadCapList	DisableMouseCapture	AddAutoFTPToDB


It seems like you are trying to set up a C&C server.
Would you like help?
Yes
No

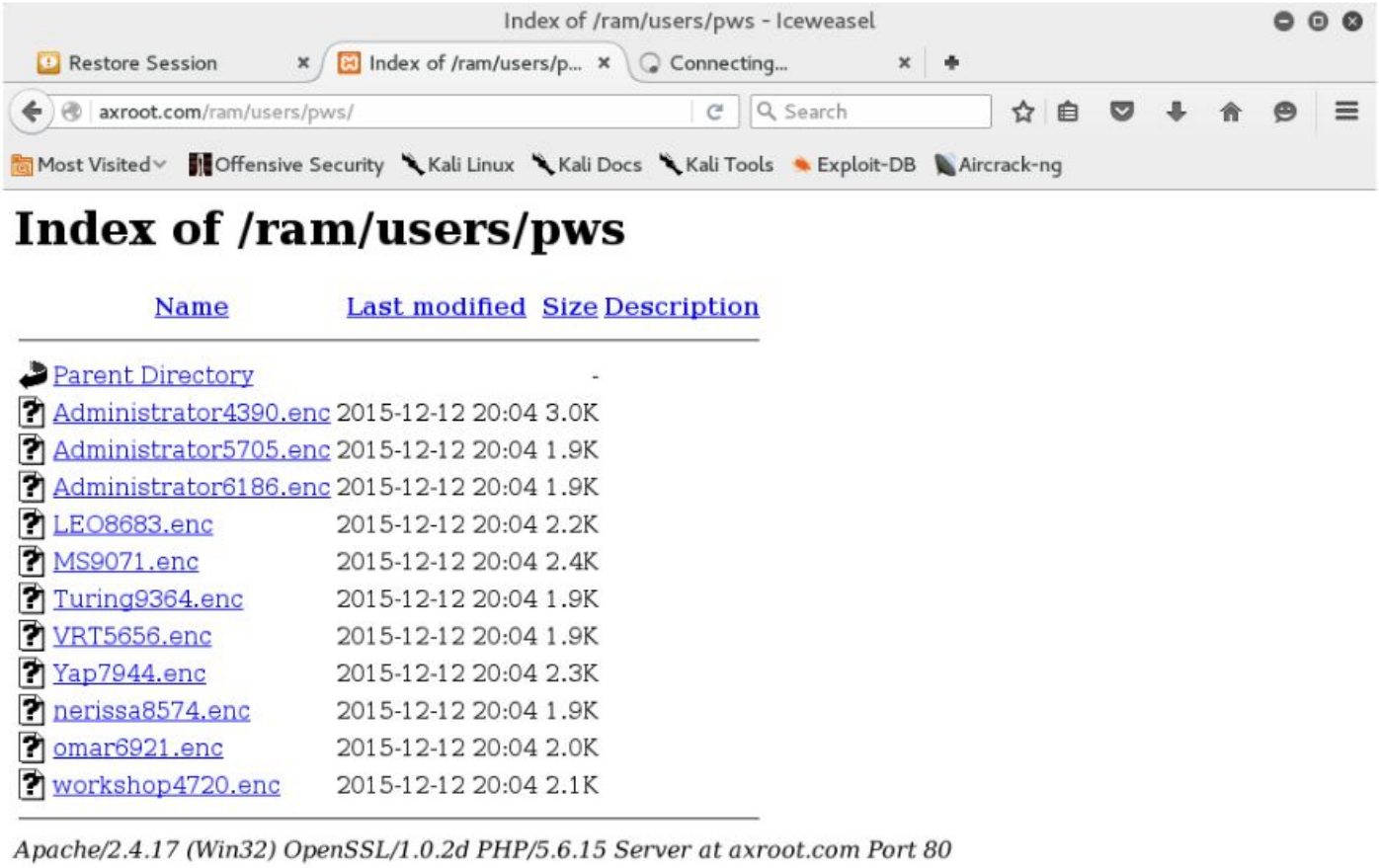


Fig 10. Uploaded password files from other victims

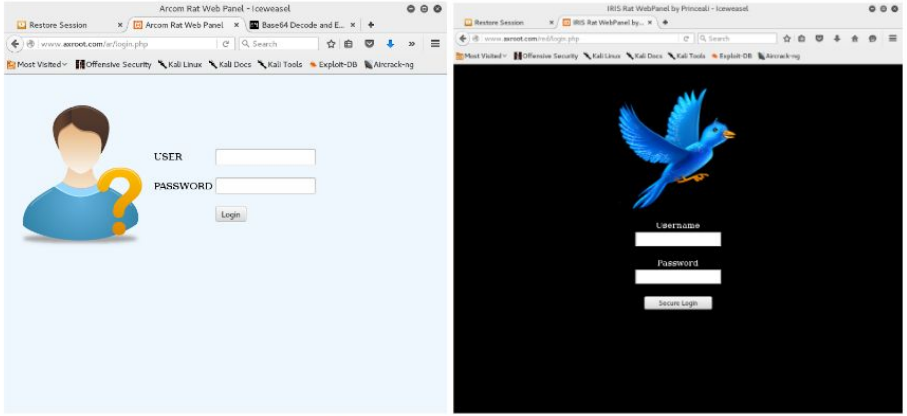


Fig 11. Web based RAT control panels found on Operation Manul C2 Servers

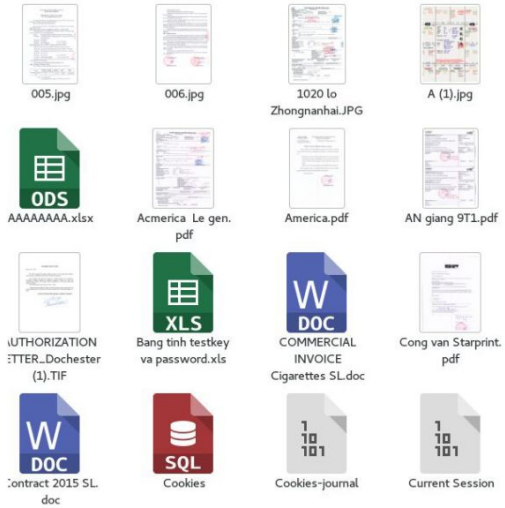


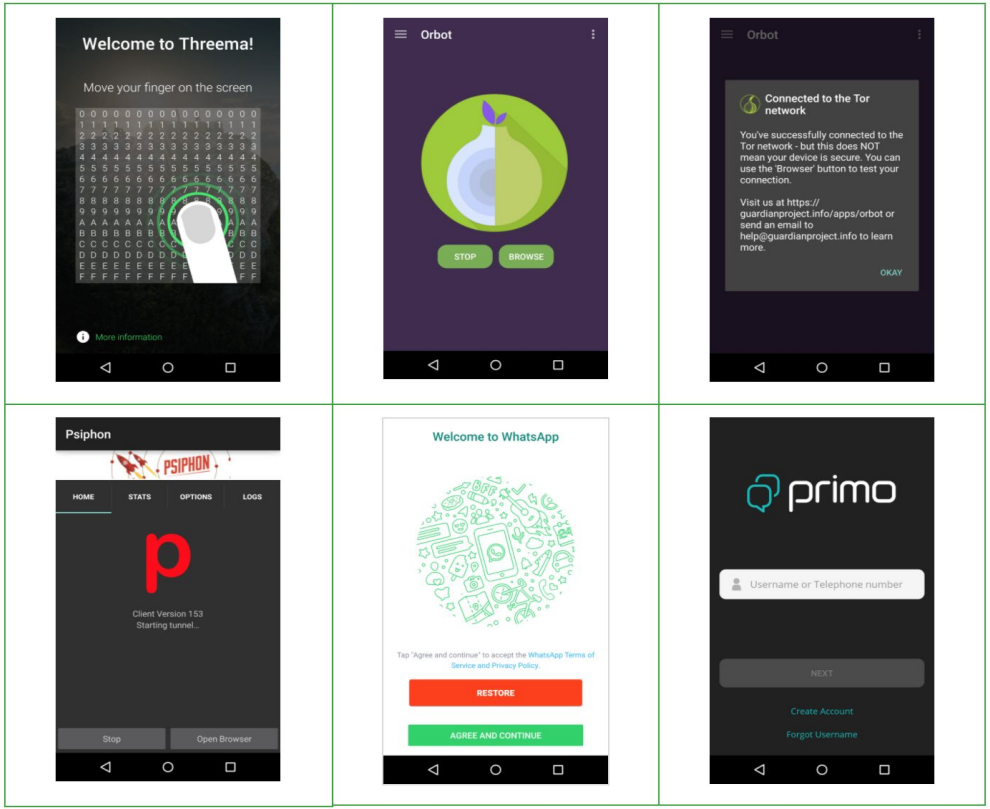
Fig 12. Uploaded documents from the victim of another campaign found on Operation Manul servers.

Dark Caracal - Pallas



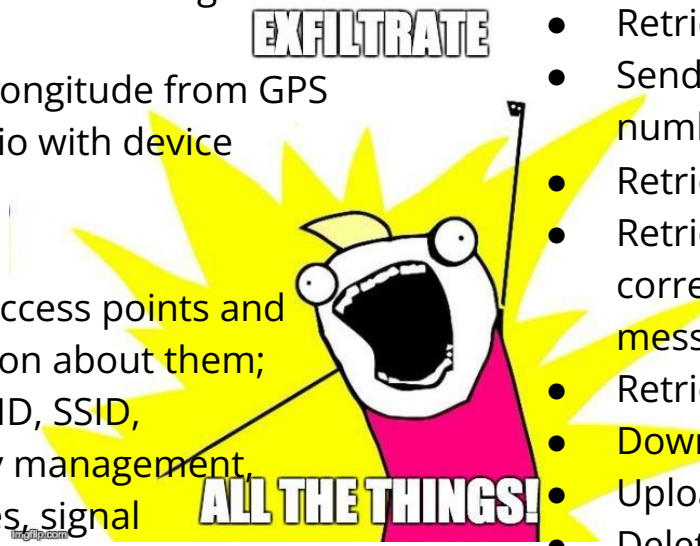
Pallas

- **Secure messaging**
  - Threema, Signal, WhatsApp, Primo, Plus Messenger
- **Privacy / Connectivity**
  - Orbot, Psiphon
- **Miscellaneous**
  - Flash Player, Google Play Push
- **Most are fully functional**

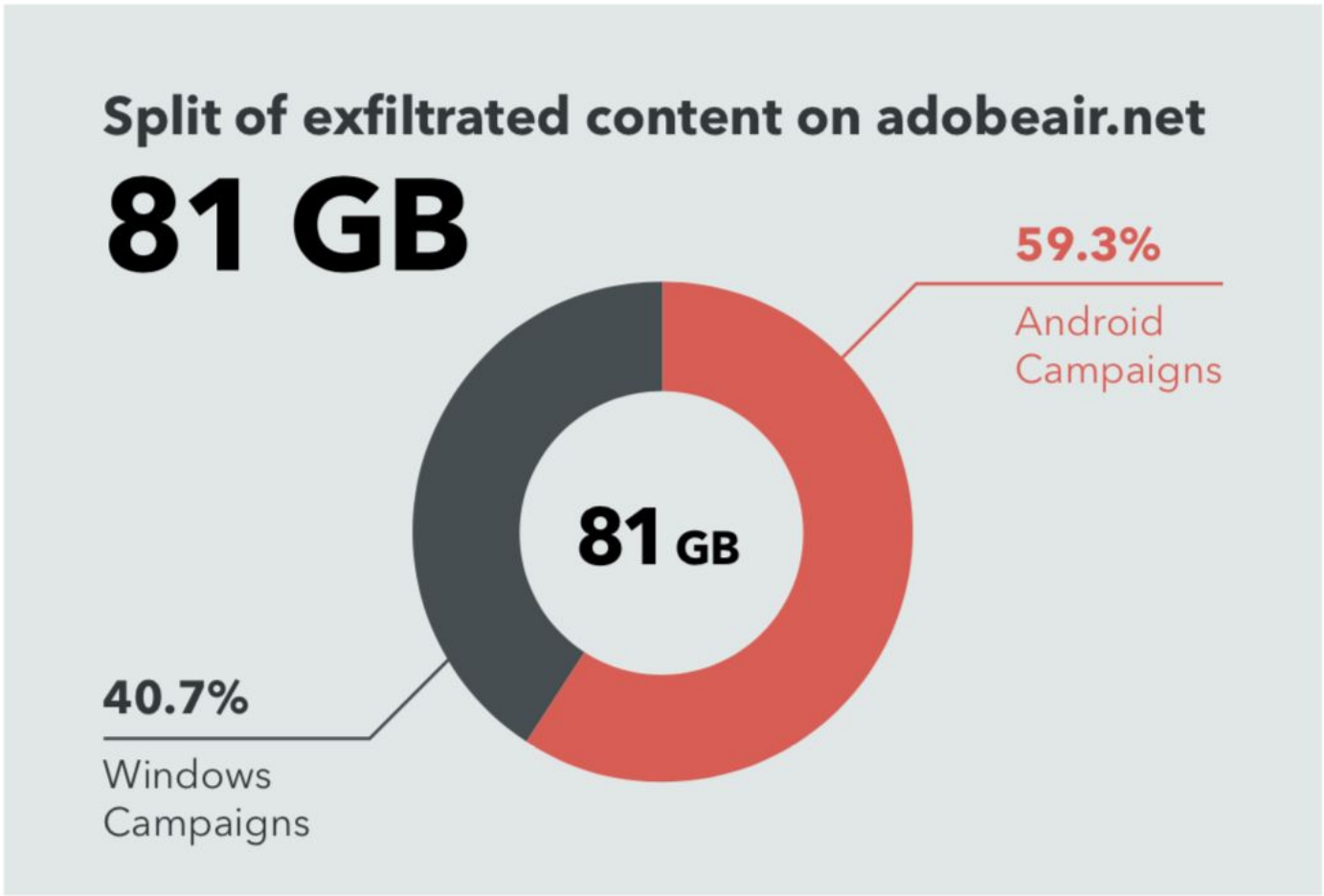


Pallas

- Take photos with front or back camera
- Intercept incoming text messages and exfiltrate
- Retrieve latitude / longitude from GPS
- Silently record audio with device microphone
- Retrieve contacts
- Scan nearby WIFI access points and exfiltrate information about them; including their BSSID, SSID, authentication, key management, encryption schemes, signal strength, and frequency

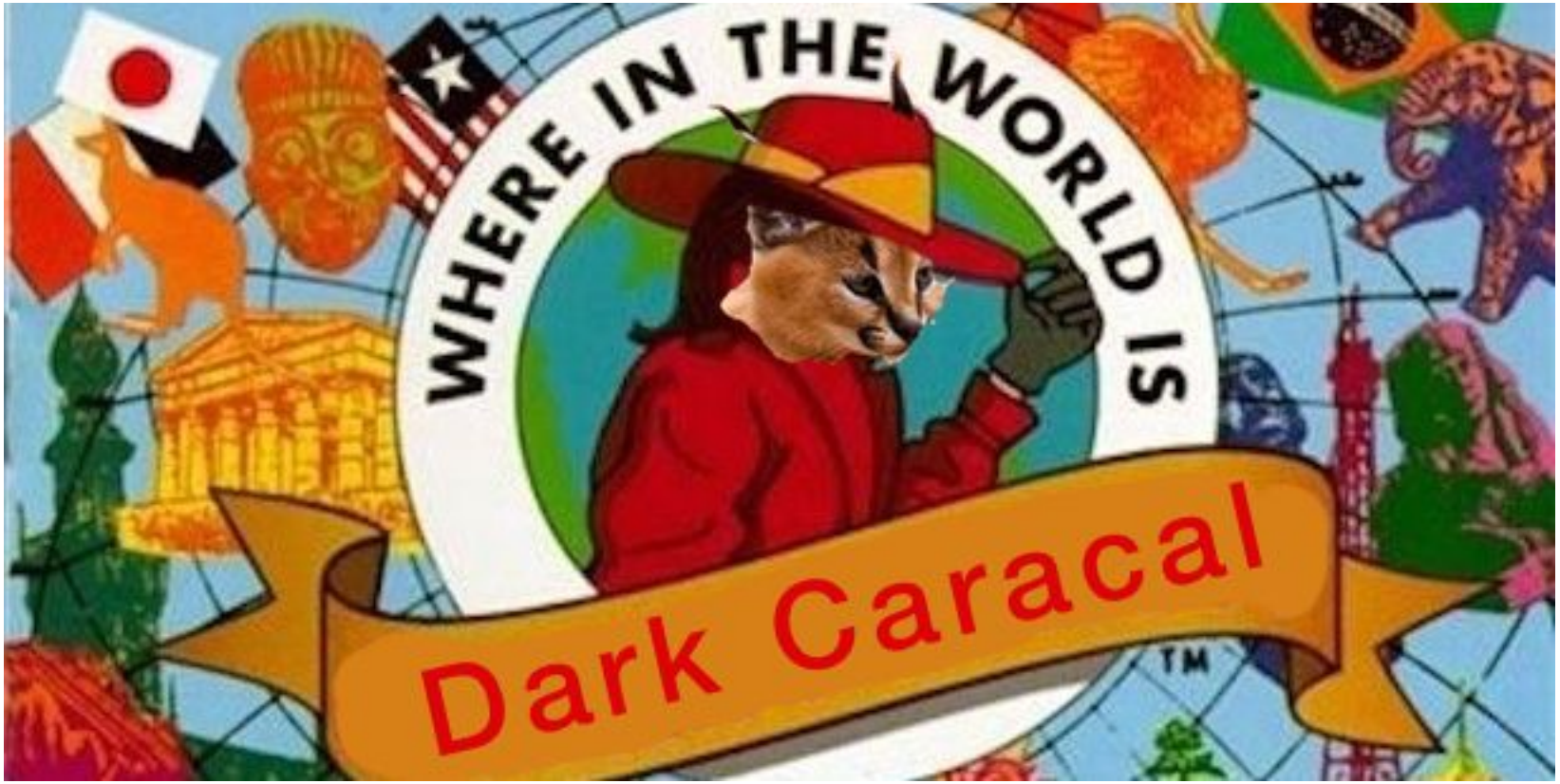


- Retrieve device metadata
- Retrieve text messages
- Retrieve information about all accounts
- Send an SMS to an attacker specified number
- Retrieve call logs
- Retrieve messages and any corresponding decryption keys from messaging apps
- Retrieve a list of installed packages
- Download and install additional apps
- Upload attacker specified files
- Delete attacker specified files and directories


Split of exfiltrated content on adobeair.net
81 GB
59.3%
Android
Campaigns
81 GB
40.7%
Windows
Campaigns

Client	Protocol	VHost	Request
	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]&pr=111111111111
	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]&pr=111111111111
	http/1.1	www.example.com:443	GET /wp9/add.php?ac=chkcm1&uid=[redacted]&pr=101111111111
	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]&pr=111111111111
	http/1.1		
	http/1.1	www.example.com:443	POST /oldb/upload.php?test=[redacted]&op=0&rn=no&extra=bla
	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]
	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]
	http/1.1	www.example.com:443	GET /wp7/add.php?ac=chkcm1&uid=[redacted]
	http/1.1	www.example.com:443	GET /oldb/add.php?ac=chkcm1&uid=[redacted]
	http/1.1		

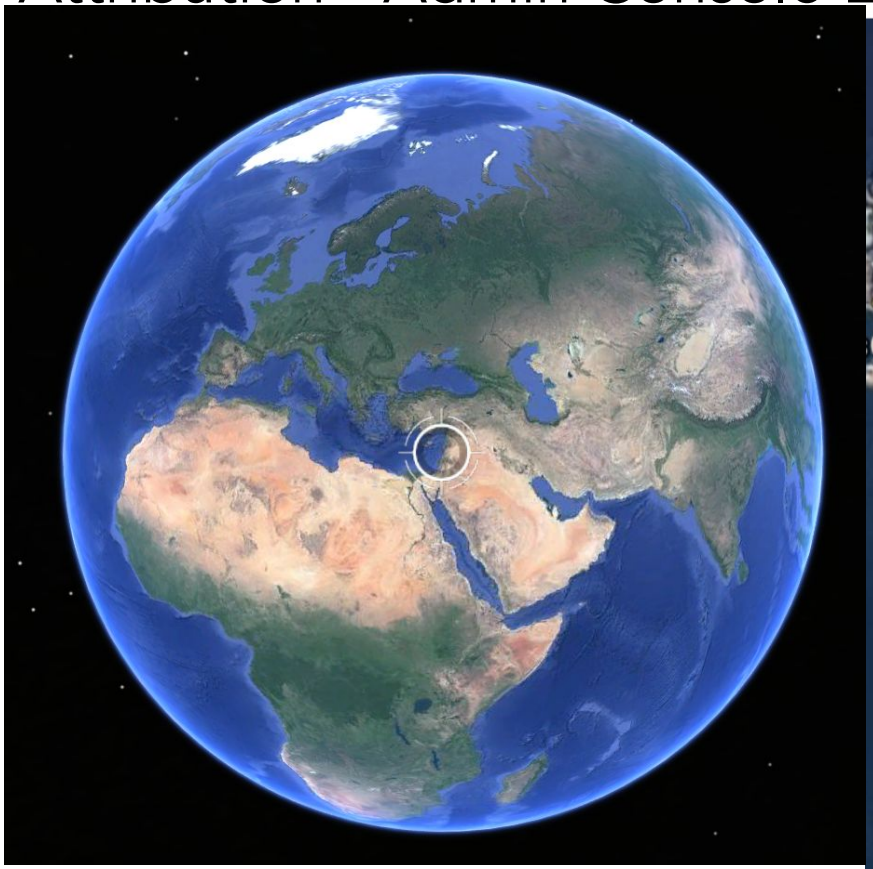


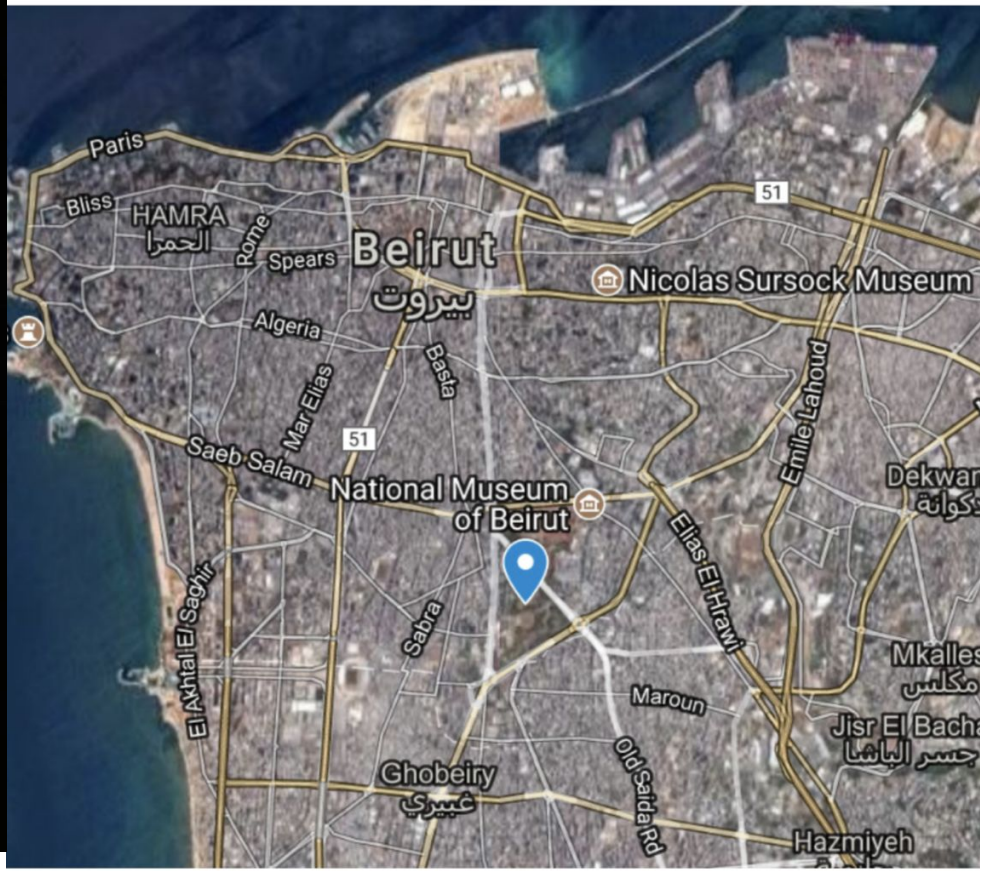

WHERE IN THE WORLD IS
Dark Caracal
TM

G

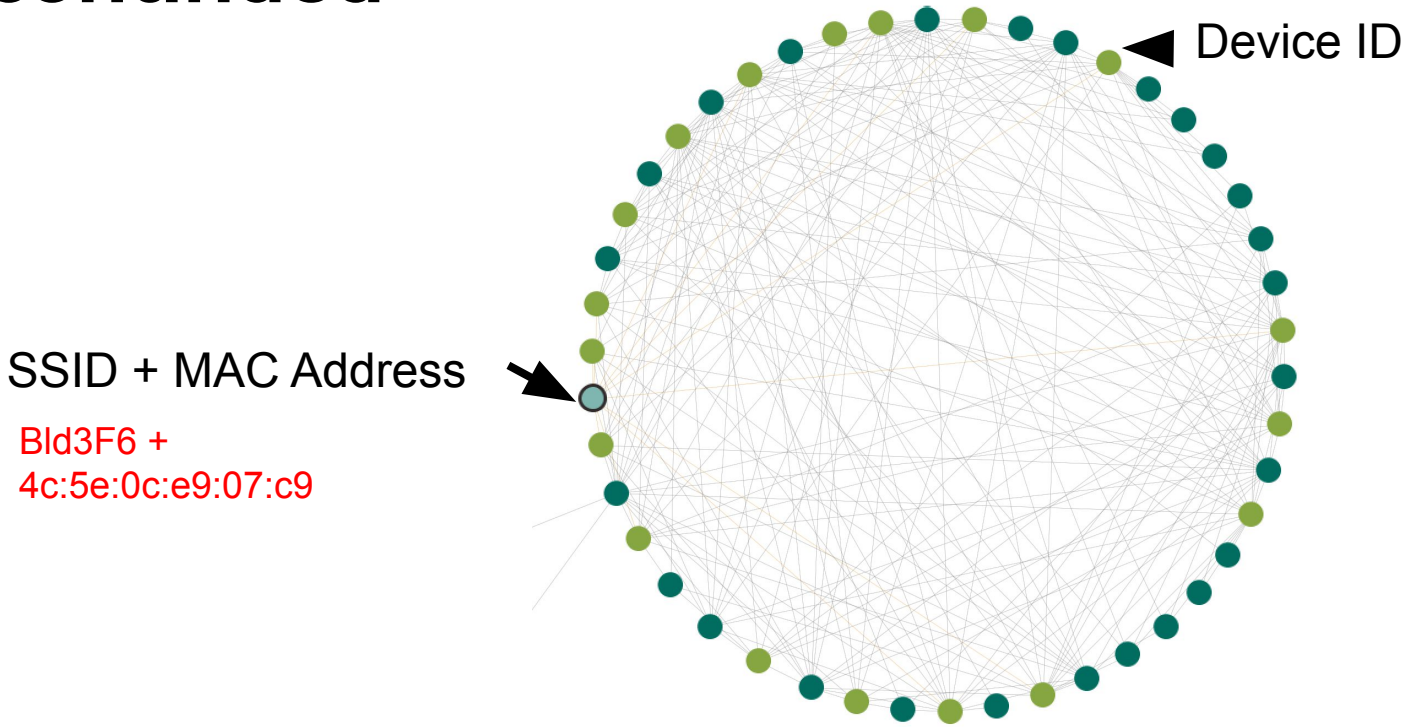


Attribution - Admin Console Logins

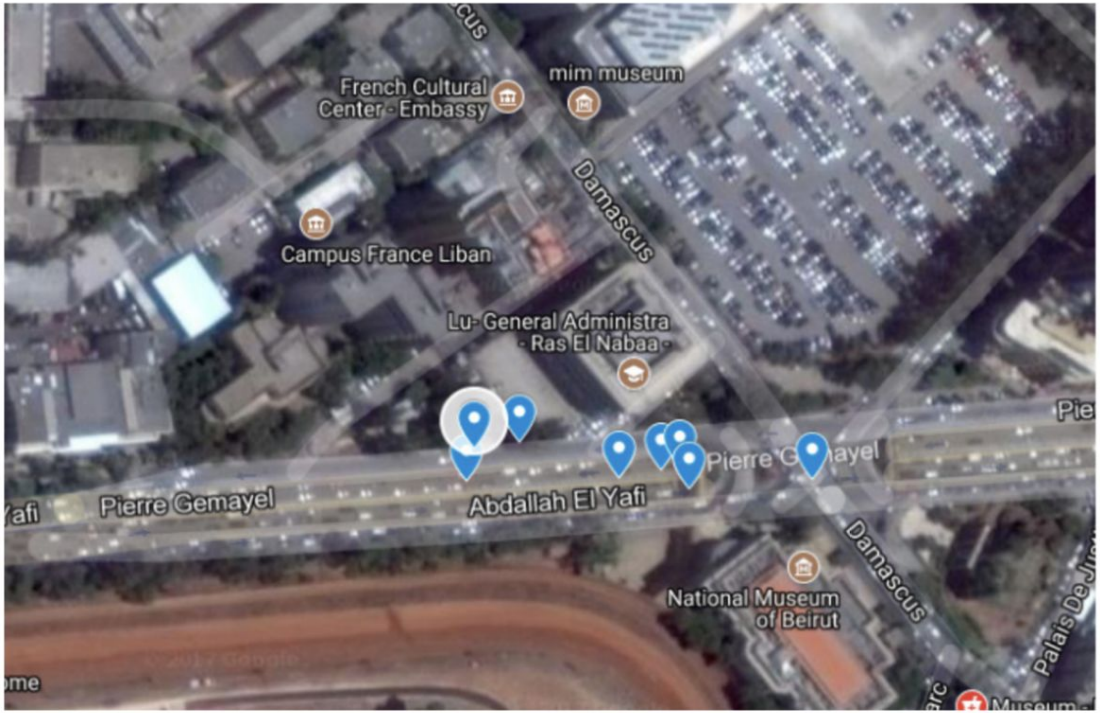


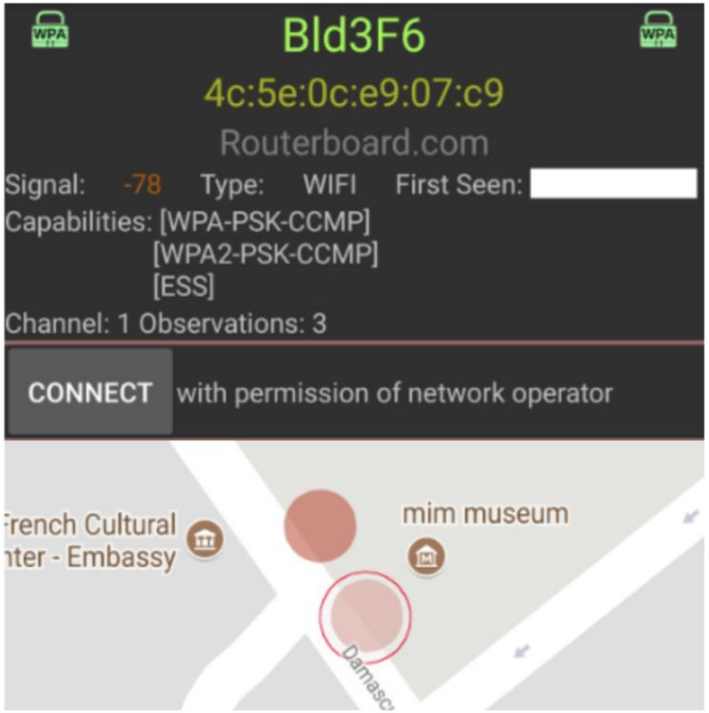


Attribution - Locating Attacker Facilities, continued

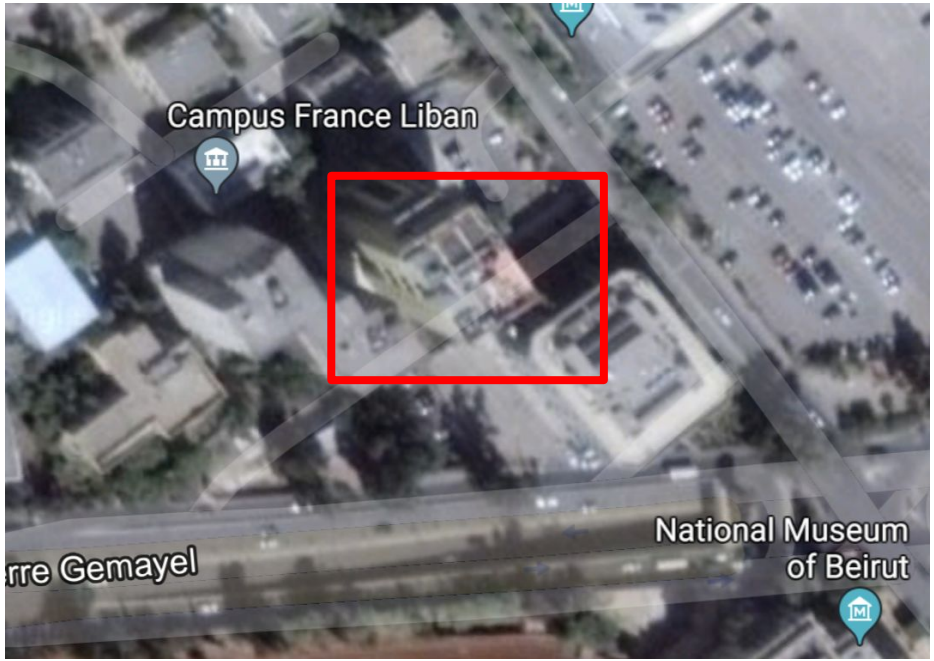


Attribution - Locating Attacker Facilities, continued





Attribution - Testing Location






$V = \frac{1}{3}\pi r^2 . h$
h
r
$y = ax^2 + bx + c$
$(x_1, x_2) = \frac{-b \pm \Delta}{2a}$
30° 45° 60°
sin $\frac{1}{2}$ $\frac{\sqrt{2}}{2}$ $\frac{\sqrt{3}}{2}$
cos $\frac{\sqrt{3}}{2}$ $\frac{\sqrt{2}}{2}$ $\frac{1}{2}$
tan $\frac{\sqrt{3}}{3}$ 1 $\sqrt{3}$
2x
60°
30°
x√3
45°
x√2
x

Bandidos at large: A spying campaign in Latin America

ESET Research uncovers an active malicious campaign that uses new versions of old malware, Bandook, to spy on its victims

BANDOOK: SIGNED & DELIVERED

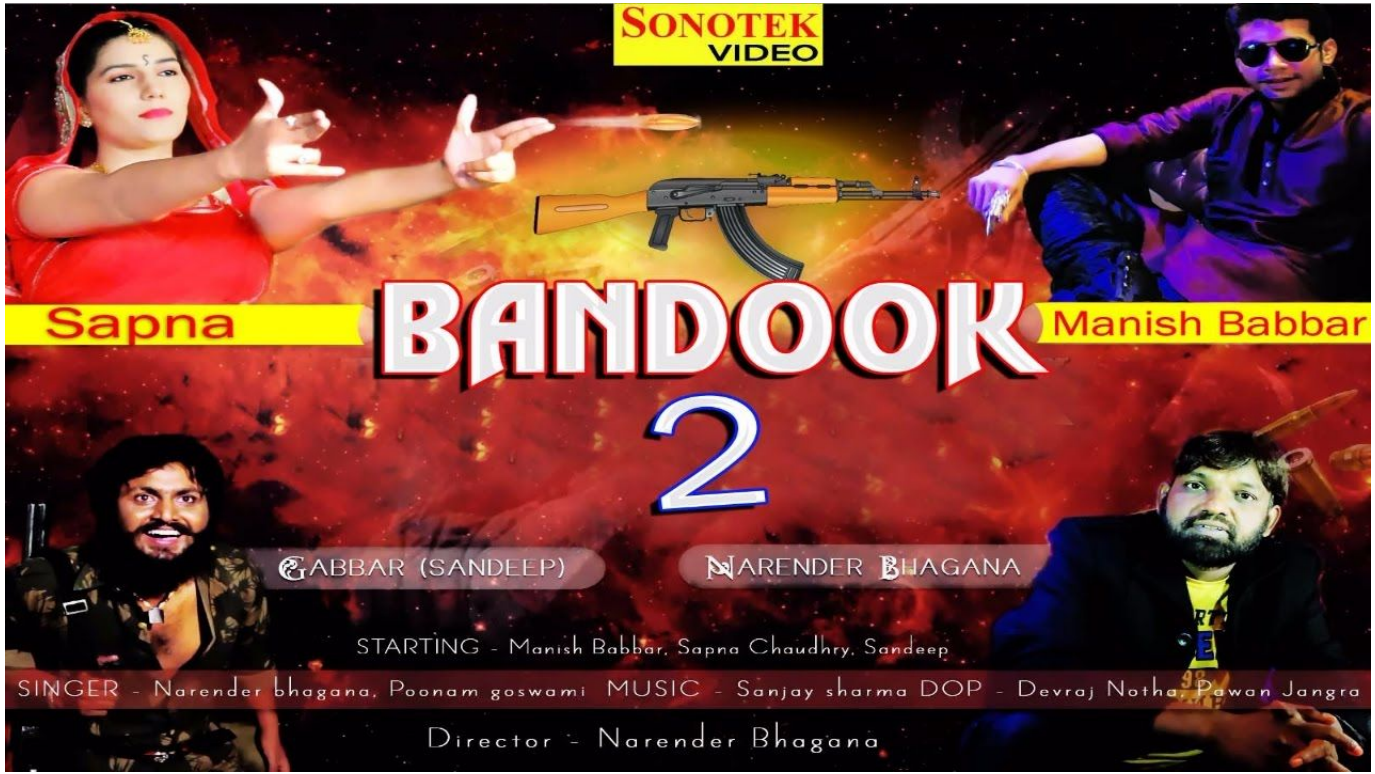
...

November 26, 2020

Introduction

Check Point Research recently observed a new wave of campaigns against various targets worldwide that utilizes a strain of a 13-year old backdoor Trojan named Bandook.

2022: A New Bandook Appears



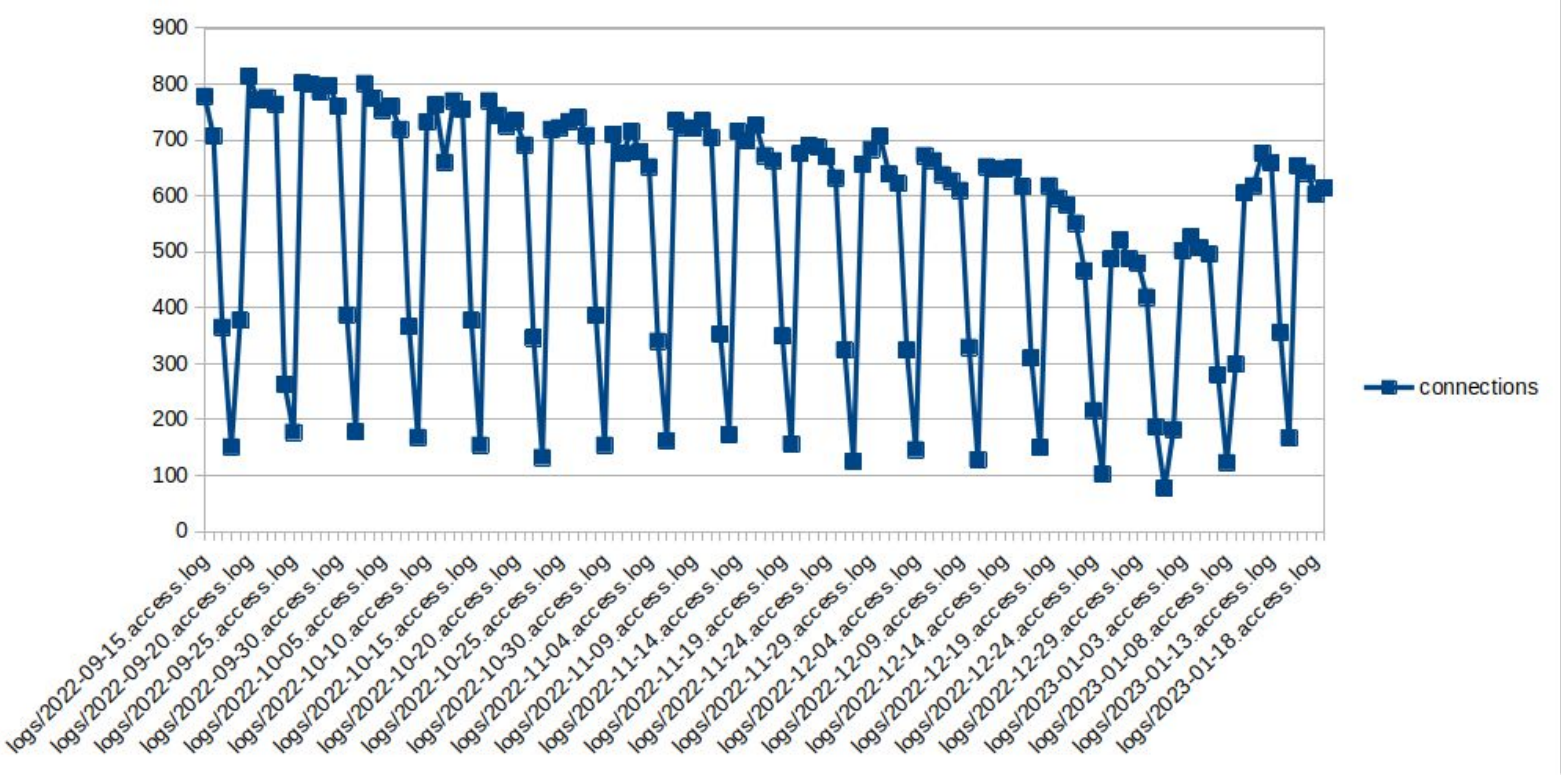
```
$~ whois unclesow.com
No match for domain "UNCLESOW.COM".
```

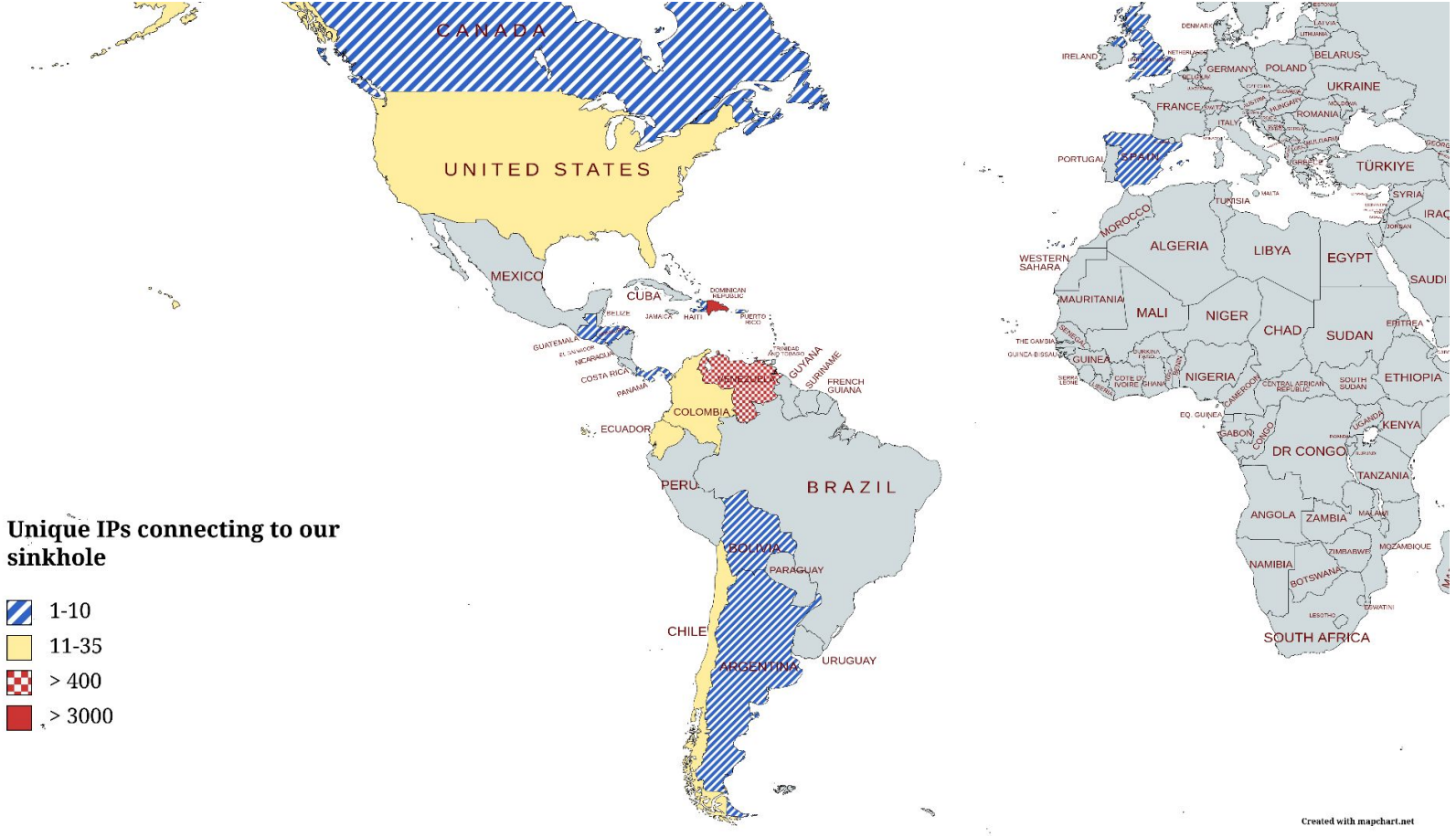


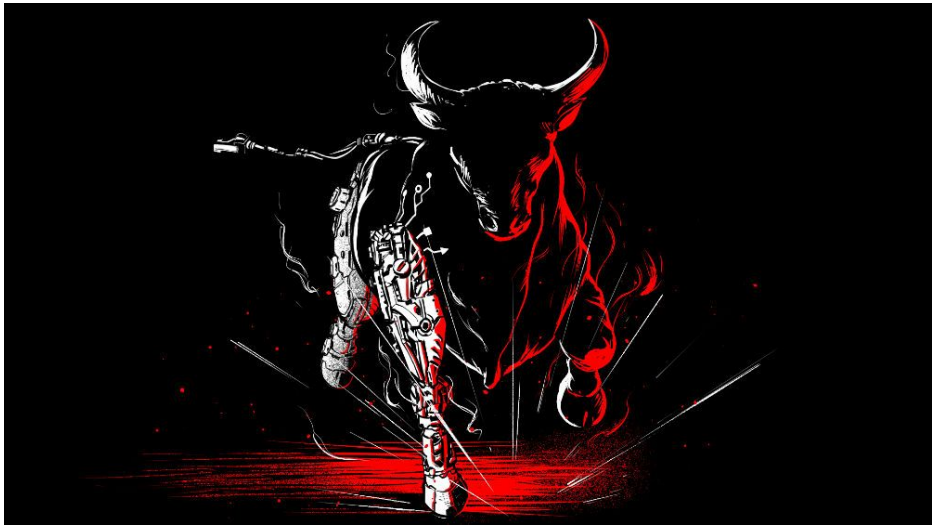


unclesow.com

This domain is a malware sinkhole operated by The Electronic Frontier Foundation. It logs data as described by our privacy policy
This is not a malicious domain but if your computer is connecting to it you may be infected with the Bandook malware.
For questions or comments please email info@eff.org.




CANADA
UNITED STATES
MEXICO
CUBA
DOMINICAN REPUBLIC
HAITI
JAMAICA
BELIZE
GUATEMALA
EL SALVADOR
NICARAGUA
COSTA RICA
PANAMA
VENEZUELA
GUYANA
SURINAME
FRENCH GUIANA
COLOMBIA
ECUADOR
PERU
BRAZIL
BOLIVIA
PARAGUAY
CHILE
ARGENTINA
URUGUAY
Unique IPs connecting to our sinkhole
1-10
11-35
> 400
> 3000
IRELAND
DENMARK
NETHERLANDS
BELGIUM
GERMANY
POLAND
BELARUS
UKRAINE
FRANCE
ROMANIA
ITALY
PORTUGAL
SPAIN
TÜRKIYE
MALTA
TUNISIA
SYRIA
MOROCCO
ALGERIA
LIBYA
EGYPT
WESTERN SAHARA
MAURITANIA
MALI
NIGER
CHAD
SUDAN
ERITREA
SAUDI
GUINEA
NIGERIA
ETHIOPIA
CENTRAL AFRICAN REPUBLIC
SOUTH SUDAN
EQ. GUINEA
GABON
CONGO
DR CONGO
KENYA
TANZANIA
ANGOLA
ZAMBIA
NAMIBIA
BOTSWANA
ZIMBABWE
MOZAMBIQUE
SOUTH AFRICA
Created with mapchart.net



CONTI


D


NSO GROUP
DARKMATTER
DARK CARACAL
imgflip.com

Conclusions

- Despite the number of mistakes they have made, Dark Caracal is still disturbingly effective.
- The number of cyber mercenaries is growing, and there is a spectrum, not everyone is a high end player
- IMO this growth is due to how successful encryption has been, web encryption is ubiquitous, E2EE is nearly there as well
- This means that governments are increasingly hacking individual devices to spy on people
- Encryption was the fight of the last 30 years, and we are winning. Spyware is the next battle

Thank You! Questions?