



ALL YOUR PLAINTEXT ARE BELONG TO US

All Your Plaintext Are Belong To Us: How the Mercenary Spyware Industry Helps Governments Circumvent Encryption

Bill Marczak





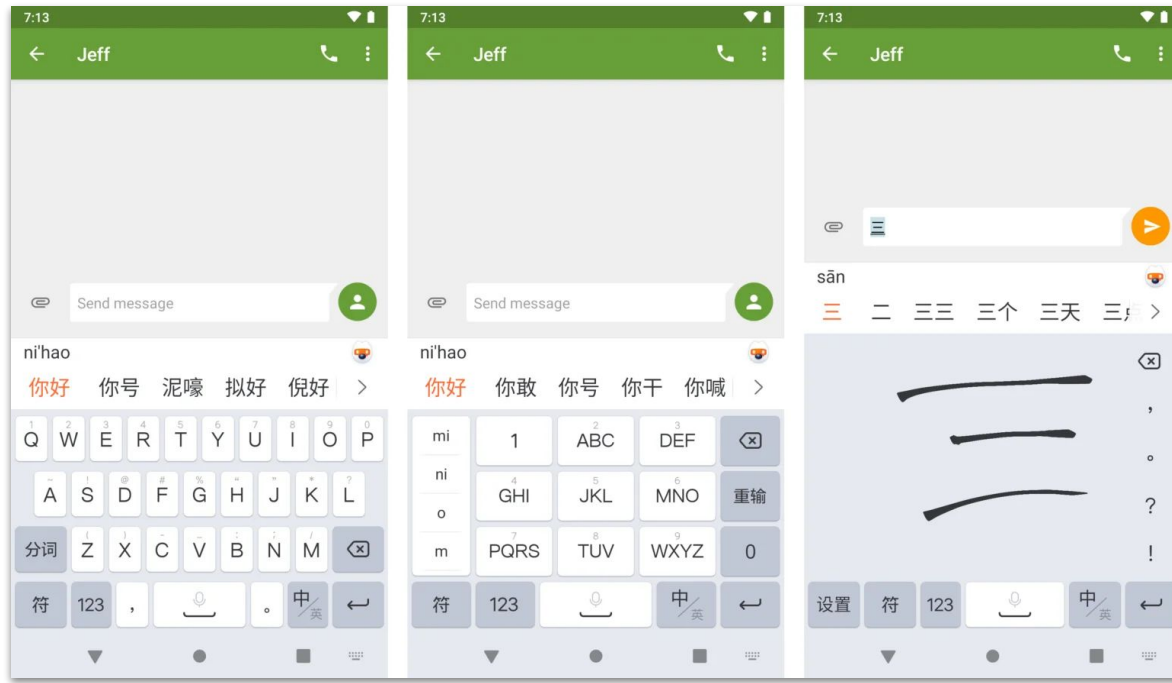


Study novel technological threats to human rights



Study novel technological threats to human rights

"Targeted Threats": spyware, hacking, ...



We found that each version of Sogou Input Method encrypts sensitive data using an encryption system that is internally referred to as the “EncryptWall” encryption system. We found that the Windows and Android versions of Sogou Input Method contain vulnerabilities in this encryption system, including a vulnerability to a [CBC padding oracle attack](#), which allow



“Please do not make it public”

Vulnerabilities in Sogou Keyboard encryption expose keypresses to network eavesdropping

By Jeffrey Knockel, Zoë Reichert, and Mona Wang

August 9, 2023

[阅读简体中文摘要](#) | [閱讀繁體中文摘要](#)

tion system that is internally referred to as the “EncryptWall” encryption system. We found that the Windows and Android versions of Sogou Input Method contain vulnerabilities in this encryption system, including a vulnerability to a [CBC padding oracle attack](#), which allow

Proposition 1

If you're a government* with a checkbook

Proposition 1

If you're a government* with a checkbook

* (employee, contractor, head-of-state, "know a guy", etc.)

Proposition 1

If you're a government* with a checkbook

* (employee, contractor, head-of-state, "know a guy", etc.)

Then you can pwn a device if it visits a URL you control

Proposition 1

If you're a government* with a checkbook

* (employee, contractor, head-of-state, "know a guy", etc.)

Then you can pwn a device if it visits a URL you control

- Target clicks on a link in message
- Target's browser fetches malicious ad
- Target web request tampered with

Proposition 1

If you're a government* with a checkbook

* (employee, contractor, head-of-state, "know a guy", etc.)

Then you can pwn a device if it visits a URL you control

- Target clicks on a link in message
- Target's browser fetches malicious ad
- Target web request tampered with

~24/7/365
All Popular Devices

Proposition 2

If you're a government* with a (bigger) checkbook

* (employee, contractor, head-of-state, "know a guy", etc.)

Proposition 2

If you're a government* with a (bigger) checkbook

* (employee, contractor, head-of-state, "know a guy", etc.)

Then you can pwn a device by "push"

- **Serialization bugs (e.g., XML, NSKeyedArchive)**
- **Malicious attachment (e.g., PDF, WebP)**

Proposition 2

If you're a government* with a (bigger) checkbook

* (employee, contractor, head-of-state, "know a guy", etc.)

Then you can pwn a device by "push"

- Serialization bugs (e.g., XML, NSKeyedArchive)
- Malicious attachment (e.g., PDF, WebP)

"Sometimes"
Some Devices

What is "Mercenary Spyware"?

From: Melissa Chan <melissa.aljazeera@gmail.com>


To:


Sent: Tuesday, 8 May 2012, 8:52

Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights
Bahrain reports of torture on Mr. Nabeel Rajab after his recent
arrest.

Please check the attached detailed report along with torture
images.

▶  1 attachment: Rajab.rar 1.4 MB

 Save

From: Melissa Chan <melissa.aljazeera@gmail.com>

To:

Sent: Tuesday, 8 May 2012, 8:52

Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights
Bahrain reports of torture on Mr. Nabeel Rajab after his recent
arrest.

Please check the attached detailed report along with torture
images.

1 attachment: Rajab.rar 1.4 MB

Save



exe.Rajab.jpg

From: Melissa Chan <melissa.aljazeera@gmail.com>

To:

Sent: Tuesday, 8 May 2012, 8:52

Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights
Bahrain reports of torture on Mr. Nabeel Rajab after his recent
arrest.

Please check the attached detailed report along with torture
images.



exe.Rajab.jpg

1 attachment: Rajab.rar 1.4 MB

Save

RIGHT-TO-LEFT OVERRIDE

Codepoint

U+202E

From: Melissa Chan <melissa.aljazeera@gmail.com>

To:

```
S
S
V
E
a
P
ir
>
00003960 47 4e 55 20 4d 50 3a 20 43 61 6e 6e 6f 74 20 61 |GNU MP: Cannot a|
00003970 6c 6c 6f 63 61 74 65 20 6d 65 6d 6f 72 79 20 28 |llocate memory (|
00003980 73 69 7a 65 3d 25 75 29 0a 00 00 00 47 4e 55 20 |size=%u)...GNU |
00003990 4d 50 3a 20 43 61 6e 6e 6f 74 20 72 65 61 6c 6c |MP: Cannot reall|
000039a0 6f 63 61 74 65 20 6d 65 6d 6f 72 79 20 28 6f 6c |ocate memory (ol|
000039b0 64 5f 73 69 7a 65 3d 25 75 20 6e 65 77 5f 73 69 |d_size=%u new_si|
000039c0 7a 65 3d 25 75 29 0a 00 79 3a 5c 6c 73 76 6e 5f |ze=%u)..y:\lsvn |
000039d0 62 72 61 6e 63 68 65 73 5c 66 69 6e 73 70 79 76 |branches\finspyv|
000039e0 34 2e 30 31 5c 66 69 6e 73 70 79 76 32 5c 73 72 |4.01\finspyv2\sr|
000039f0 63 5c 6c 69 62 73 5c 6c 69 62 67 6d 70 5c 6d 70 |c\libs\libgmp\mp|
00003a00 6e 2d 74 64 69 76 5f 71 72 2e 63 00 63 20 3d 3d |n-tdiv_qr.c.c ==|
00003a10 20 30 00 00 00 00 00 00 01 02 03 03 04 04 04 04 |0.....
```

RIGHT-TO-LEFT OVERRIDE

Codepoint

U+202E



FinFisher Product Overview

FinSpy





Accessed Files

- Record files when they are being accessed.
Module Size: 12 KB



Changed Files

- Record files when they are being modified.
Module Size: 10 KB



Deleted Files

- Record files that are being deleted.
Module Size: 10 KB



Forensics Tools

- Provide tools to gather information from the target.
Module Size: 11 KB



Printer

- Records the printed documents.
Module Size: 12 KB



Skype

- Record all Skype calls, chats and file-transfers.
Module Size: 179 KB



Microphone

- Enable microphone recordings on Target System.
Module Size: 167 KB



Command Shell

- Remotely access the command shell.
Module Size: 7 KB



File Access

- Provide live access to the Target filesystem.
Module Size: 12 KB



Keylogger

- Record all keys that are pressed on the Target System.
Module Size: 22 KB



Scheduler

- Schedule background recordings of several modules.
Module Size: 7 KB



Screen & Webcam

- Record images from the webcam and screen.
Module Size: 12 KB



The **challenges** in today's communication technology are based on these facts:



Higher security standards

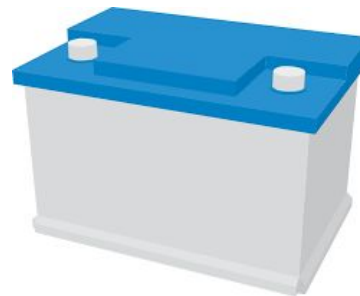
FinFisher™ partners exclusively with Law Enforcement and Intelligence Agencies, being your reliable partner and trusted advisor to effectively **prevent and investigate terror and crime.**



Martin Muench
Head of FinFisher (Fmr.)



"GIVEN THAT A CAN OF FIZZY DRINK OR A CAR BATTERY CAN BE ABUSED AND USED AS AN IMPLEMENT OF TORTURE IT IS OF NO SURPRISE TO ANYONE IF OUR PRODUCTS CAN BE ABUSED TOO."





MOTHERBOARD

TECH BY VICE

A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher

A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher

Android Trojan
Generation error

Unable to generate Trojan for Android mobile devices. Received this error while attempting it

A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher

Android Trojan
Generation error

Unable to generate Trojan for Android mobile devices. Received this error while attempting it

The problem has been fixed during a **Skype session**.
The binary was exchanged accordingly.

A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher

Android Trojan
Generation error

Unable to generate Trojan for Android mobile devices. Received this error while attempting it

The problem has been fixed during a Skype session. The binary was exchanged accordingly.

should work but not working

Hi, its Arefin from Bangladesh. yesterday we have infected one target. He is online showed by the agent but we are not getting any feeding from him. Moreover, we have that confirmation that the person is in online and doing some activity. **Please reply with suggestions** Regards

A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher

Android Trojan
Generation error

Unable to generate Trojan for Android mobile devices. Received this error while attempting it

The problem has been fixed during a Skype session. The binary was exchanged accordingly.

should work but not working

Hi, its Arefin from Bangladesh. yesterday we have infected one target. He is online showed by the agent but we are not getting

The infection rate is practically zero percent

Since the **release of the new version** i.e. 4.1 the trojan is unable to infect any target. There is absolutely no response from any of the targets we attacked. **Plz look in to this matter** as it is very serious one.

A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher

Android Trojan
Generation error

Unable to generate Trojan for Android mobile devices. Received this error while attempting it

The problem has been fixed during a Skype session. The binary was exchanged accordingly.

should work but not working

Hi, its Arefin from Bangladesh. yesterday we have infected one target. He is online showed by the agent but we are not getting

The infection rate is practically zero percent

Since the release of the new version i.e. 4.1 the trojan is unable to infect any target. There is absolutely no response from any of the targets we attacked. Plz look in to this matter

as it is Enquiry on how to copy a executable and run it on an infected computer

I have a target which the computer is already infected with finspy. Would like to check **is there any way which I could upload an executable to the target computer** and then execute it?

ID	Software	System	AV	Empty Trojan			Full Trojan			Empty Vista W7 USER Infection			Full Vista W7 USER Infection			MBR Full Trojan		File Infection (*.jpg)		Executable (*.exe)		Word (*.doc)			
			Support	Install Admin	Install User	Scan	Install Admin	Install User	Scan	Install Admin	Install User	Scan	Install Admin	Install User	Scan	Install Admin	Scan	Install Admin	Scan	Install Admin	Scan	Install Admin	Scan	Install Admin	Scan
AV23	Panda Global Protection 2014	XP	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	fail	fail	fail	fail	pass	pass	pass	pass
AV24	Q																								
AV25	Se																								
AV26	Sophos Endpoint Security and Control	W8(64bit)		pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		XP	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
AV27	TotalDefense	XP	yes	warn	pass	pass	warn	pass	pass	pass	pass	pass	pass	pass	pass	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass
		W7(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
AV28	Trend Micro Titanium Maximum Security 2014	XP	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
AV29	TrustPort Total Security	XP	yes	warn	warn	pass	warn	warn	pass	pass	pass	pass	pass	pass	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass	pass
		W7(32bit)	yes	warn	pass	pass	warn	pass	pass	warn	warn	pass	warn	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass
		W7(64bit)	yes	warn	pass	pass	warn	pass	pass	warn	warn	pass	warn	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass
		W8(32bit)	yes	warn	pass	pass	warn	pass	pass	warn	warn	pass	warn	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass
		W8(64bit)	yes	warn	pass	pass	warn	pass	pass	warn	warn	pass	warn	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass
AV30	Vibre Internet Security 2014	XP	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
AV31	Zone Alarm Extreme Security	XP	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass

Detected by Avira Antivirus

The infection is detectable by the Avira Antivirus on target machine. This happened in a

ID	Software	System	AV	Empty Trojan			Full Trojan			Empty Vista W7 USER Infection			Full Vista W7 USER Infection			MBR Full Trojan		File Infection (*.jpg)		Executable (*.exe)		Word (*.doc)		
			Support	Install Admin	Install User	Scan	Install Admin	Install User	Scan	Install Admin	Install User	Scan	Install Admin	Install User	Scan	Install Admin	Scan	Install Admin	Scan	Install Admin	Scan	Install Admin	Scan	Install Admin
AV23	Panda Global Protection 2014	XP	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	fail	fail	fail	fail	pass	pass	pass	pass
AV24	Q																							
AV25	Se																							
AV26	Sophos End																							
AV27	TotalDefens																							
AV28	Trend Micro																							
AV29	TrustPort To																							
AV30	Vibre Internet Security 2014	W8(64bit)	yes	warn	pass	warn	pass	warn	pass	warn	warn	pass	warn	warn	pass	warn	pass	warn	pass	warn	pass	warn	pass	warn
AV31	Zone Alarm Extreme Security	XP	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W7(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(32bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
		W8(64bit)	yes	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass

Detected by Avira Antivirus

The infection is detectable by the Avira Antivirus on target

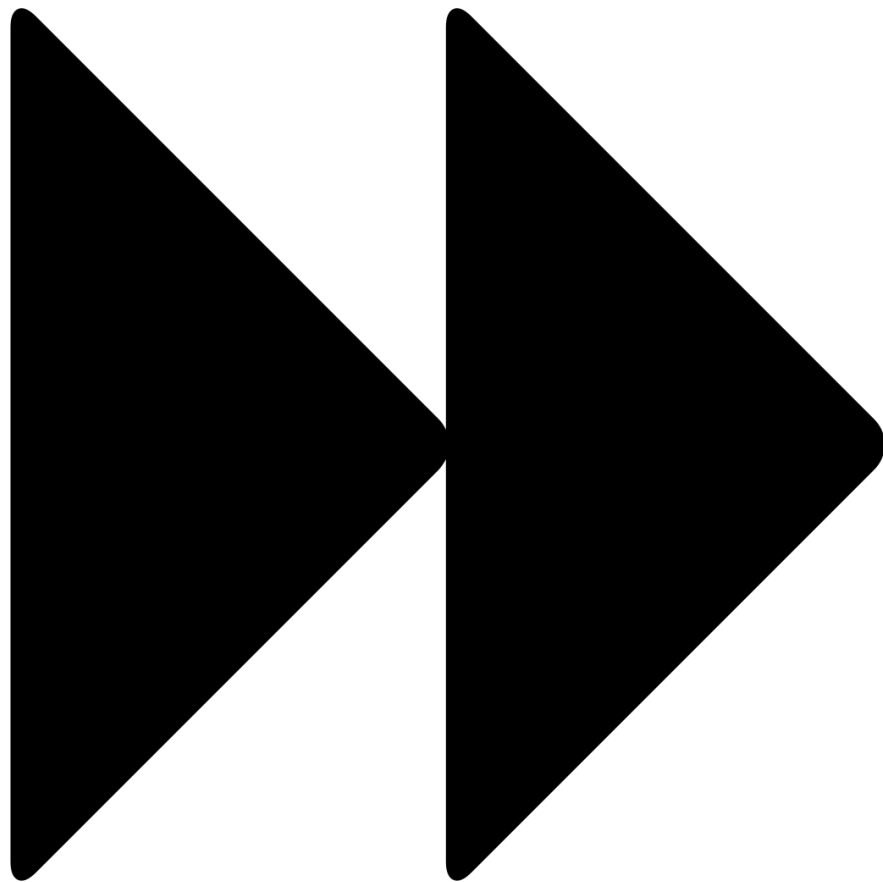
detection

AVAST detects executed exe as infection Software version: Win7_64, AVAST2014 free version infection usermode UAC bypass., empty troj. without modules

ID	Software	AV	Fmstv Trojan	Full Trojan	Fmstv Vista W7 USER Infection	Full Vista W7 USER Infection	MRR Full Trojan	File Infection (*.lnp)	Executable (*.exe)	Word (*.doc)	
										Install Admin	Scan
AV23	Panda Glot									pass	pass
										pass	pass
										pass	pass
										pass	pass
										pass	pass
AV24	Qu									pass	pass
										pass	pass
										pass	pass
										pass	pass
										pass	pass
AV25	Se									fail	fail
										fail	fail
										fail	fail
										fail	fail
										fail	fail
AV26	Sophos Em									pass	pass
										pass	pass
										pass	pass
										pass	pass
										pass	pass
AV27	TotalDefen									warn	pass
										pass	pass
										pass	pass
										pass	pass
										pass	pass
AV28	Trend Micr									pass	pass
										pass	pass
										pass	pass
										pass	pass
AV29	TrustPort 1									warn	pass
										warn	pass
										warn	pass
										warn	pass
										warn	pass
AV30	Vibre Inter									pass	pass
										pass	pass
										pass	pass
										pass	pass
										pass	pass
AV31	Zone Alarm									pass	pass
										pass	pass
										pass	pass
										pass	pass
										pass	pass

after infection,
browsers on target PC
is crashing

System: Win7_64 SP1,
Kaspersky Internet security
2014 after executing trojan PC
is infected and is sending
heartbeats to the master, but
internet browsers on target
PC- iexplorer, firefox is
crashing and user cannot open
browser. FF report error:
0xc0000005 Without
Kaspersky, browsers work
without crash.



Spyware Vendor FinFisher Claims Insolvency Amid Investigation

- Munich firm accused of helping governments hack activists
- Inquiry into alleged export controls violations ongoing

Spyware Vendor FinFisher Claims Insolvency Amid Investigation


- Munich firm accused of helping governments hack activists
- Inquiry into alleged export controls violations ongoing

German prosecutors charge four over violating trade act to sell spyware to Turkey

***SURELY THIS IS THE END
OF THE STORY, RIGHT?***

Well...

Well...



ABOUT US NEWS CONFERENCES WORK HERE


GLOBAL THREATS

Terrorists and Criminals have Gone Dark

Terrorists, drug traffickers, pedophiles, and other criminals have access to advanced technology and are harder to monitor, track, and capture than ever before.



Well...



NSO GROUP

GLOBAL THREAT

Terrorists and

Terrorists, drug traffickers,
are harder to monitor, track



Shalev Hulio

Avi Rosen

Omri Lavie



The Million Dollar Dissident

**NSO Group's iPhone Zero-Days used against a UAE
Human Rights Defender**

The Million Dollar Dissident

NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

Bitter Sweet

Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links

The Million Dollar Dissident

NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

Bitter Sweet

Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links

Part 1: [Bittersweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links](#)

Part 2: [Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware](#)

Part 3: [Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware](#)

Part 4: [Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware](#)

Part 5: [Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware](#)

Part 6: [Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware](#)

Part 7: [Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague](#)

Part 8: [Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware](#)

Peace through Pegasus

**Jordanian Human Rights Defenders and Journalists
Hacked with Pegasus Spyware**

Peace through Pegasus

**Jordanian Human Rights Defenders and Journalists
Hacked with Pegasus Spyware**

Nothing Sacred

**Religious and Secular Voices for Reform in Togo
Targeted with NSO Spyware**

Peace through Pegasus

**Jordanian Human Rights Defenders and Journalists
Hacked with Pegasus Spyware**

GeckoSpy

**Pegasus Spyware Used against Thailand's Pro-
Democracy Movement**

Nothing Sacred

**Religious and Secular Voices for Reform in Togo
Targeted with NSO Spyware**

Peace through Pegasus

**Jordanian Human Rights Defenders and Journalists
Hacked with Pegasus Spyware**

GeckoSpy

**Pegasus Spyware Used against Thailand's Pro-
Democracy Movement**

Nothing Sacred

**Religious and Secular Voices for Reform in Togo
Targeted with NSO Spyware**

Project Torogoz

**Extensive Hacking of Media & Civil Society in El
Salvador with Pegasus Spyware**

Peace through Pegasus

Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware

GeckoSpy

Pegasus Spyware Used against Thailand's Pro-Democracy Movement

CatalanGate

Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru

Nothing Sacred

Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware

Project Torogoz

Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware

Peace through Pegasus

Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware

GeckoSpy

Pegasus Spyware Used against Thailand's Pro-Democracy Movement

CatalanGate

Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru

Nothing Sacred

Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware

Project Torogoz

Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware

The Great iPwn

Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit

Peace through Pegasus

Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware

GeckoSpy

Pegasus Spyware Used against Thailand's Pro-Democracy Movement

CatalanGate

Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru

Breaking the News

New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts

Nothing Sacred

Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware

Project Torogoz

Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware

The Great iPwn

Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit

Peace through Pegasus

Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware

Nothing Sacred

Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware

GeckoSpy

Pegasus Spyware Used against Thailand's Pro-Democracy Movement

Project Torogoz

Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware

CatalanGate

Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru

The Great iPwn

Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit

Breaking the News

New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts

Pearl 2 Pegasus

Bahraini Activists Hacked with Pegasus Just Days after a Report Confirming Other Victims

UK High Court says Dubai ruler hacked ex-wife Princess Haya's phone



**Sheikh Mohammed
(Emir of Dubai)**



**Princess Haya
(his ex-wife)**



**Fiona Shackleton
(her lawyer)**

forbidden stories

🔒 PROTECT YOUR STORIES



THE PEGASUS PROJECT

LIRE EN FRANÇAIS

Well...



Shalev Hulio

Avi Rosen

Omri Lavie

"[REPORTS OF PEGASUS ABUSE] ARE HORRIBLE ... BUT THIS IS THE PRICE OF DOING BUSINESS..."

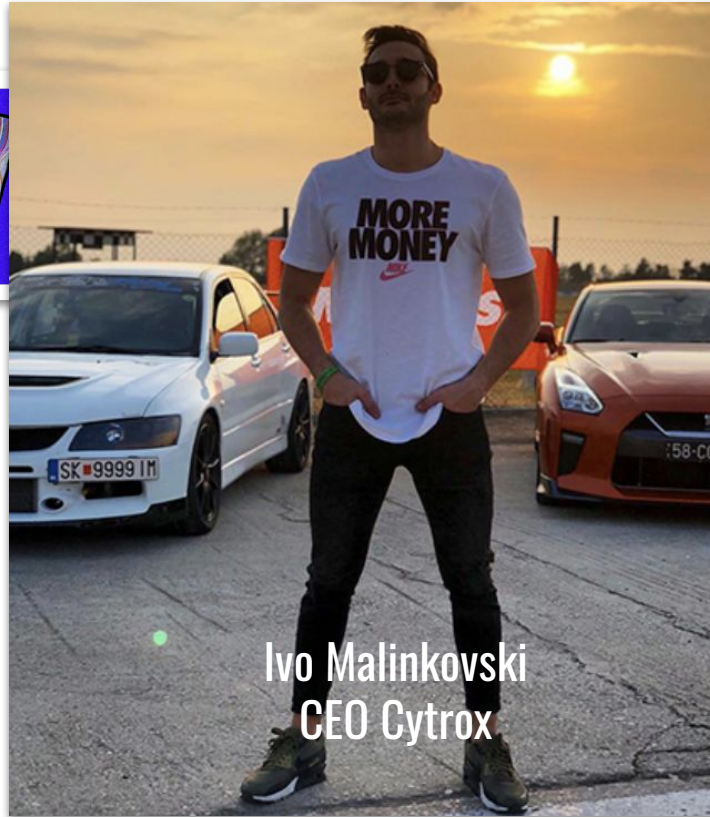
and there are other companies too!



PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions

September 22, 2023

and there are other companies too!



Ivo Malinkovski
CEO Cytrox

Why Targeted with
Identical Ambitions

and there are other companies too!



PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions

September 22, 2023



Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers

April 11, 2023

and there are other companies too!



PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions

September 22, 2023



Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers

April 11, 2023



Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus

July 15, 2021

...and more on the horizon



What is "Mercenary
Spyware"?

How do targets get
hacked in practice?

Infection techniques are evolving...

Infection techniques are evolving...



Infection techniques are evolving...

July 13
2016

Simon, my father just died
and we are devastated, I am
sending you the dates of the
wake, I hope you can come:

[\[link\]](#)

Simon amigo acaba de morir mi
padre estamos devastados, te
envio datos del velatorio espero
puedas venir:

<http://bit.ly/29xwXh5>



Infection techniques are evolving...

July 13
2016

Simon, my father just died and we are devastated, I am sending you the dates of the wake, I hope you can come:

[\[link\]](#)

Simon amigo acaba de morir mi padre estamos devastados, te envio datos del velatorio espero puedas venir:

<http://bit.ly/29xwXh5>

July 14
2016

You are an asshole Simon, while you are working I'm fking your old lady here is a photo: [\[link\]](#)

Eres un pendejo SIMON xq mientras trabajas yo me ando cogiendo a tu vieja y de prueba te mando esta foto:<http://bit.ly/29EZ50G>

Aug 11
2016

You son of a whore Simon I saw you go out with my wife do not deny it we took this photo [\[link\]](#)

Ere un hijo de tu puta madre Simon ya te vi q sales con mi esposa y no lo niegues xq te tomamos esta foto: <http://bit.ly/29EZ50G>

Aug 17
2016

Mr. Simon, [daughter's name] was just in an accident, she is in grave condition, I hope can you come, here is the where she is hospitalized: [\[link\]](#)

Sr. Simon se acaba de accidentar [nombre de su hija], esta muy grave, espero venga, le paso los datos donde esta internada: <http://bit.ly/2b2cdOM>



Infection techniques are evolving...



Infection techniques are evolving...

```
HTTP/1.1 307 Temporary Redirect  
Via: 1.0 middlebox  
Location: https://c.betly[.]me/[REDACTED]  
Connection: close
```



Infection techniques are evolving...

```
HTTP/1.1 307 Temporary Redirect
Via: 1.0 middlebox
Location: https://c.betly[.]me/[REDACTED]
Connection: close
```

CVE-2023-41993: Processing web content may lead to arbitrary code execution.

CVE-2023-41992: A local attacker may be able to elevate their privileges.

CVE-2023-41991: A malicious app may be able to bypass signature validation.

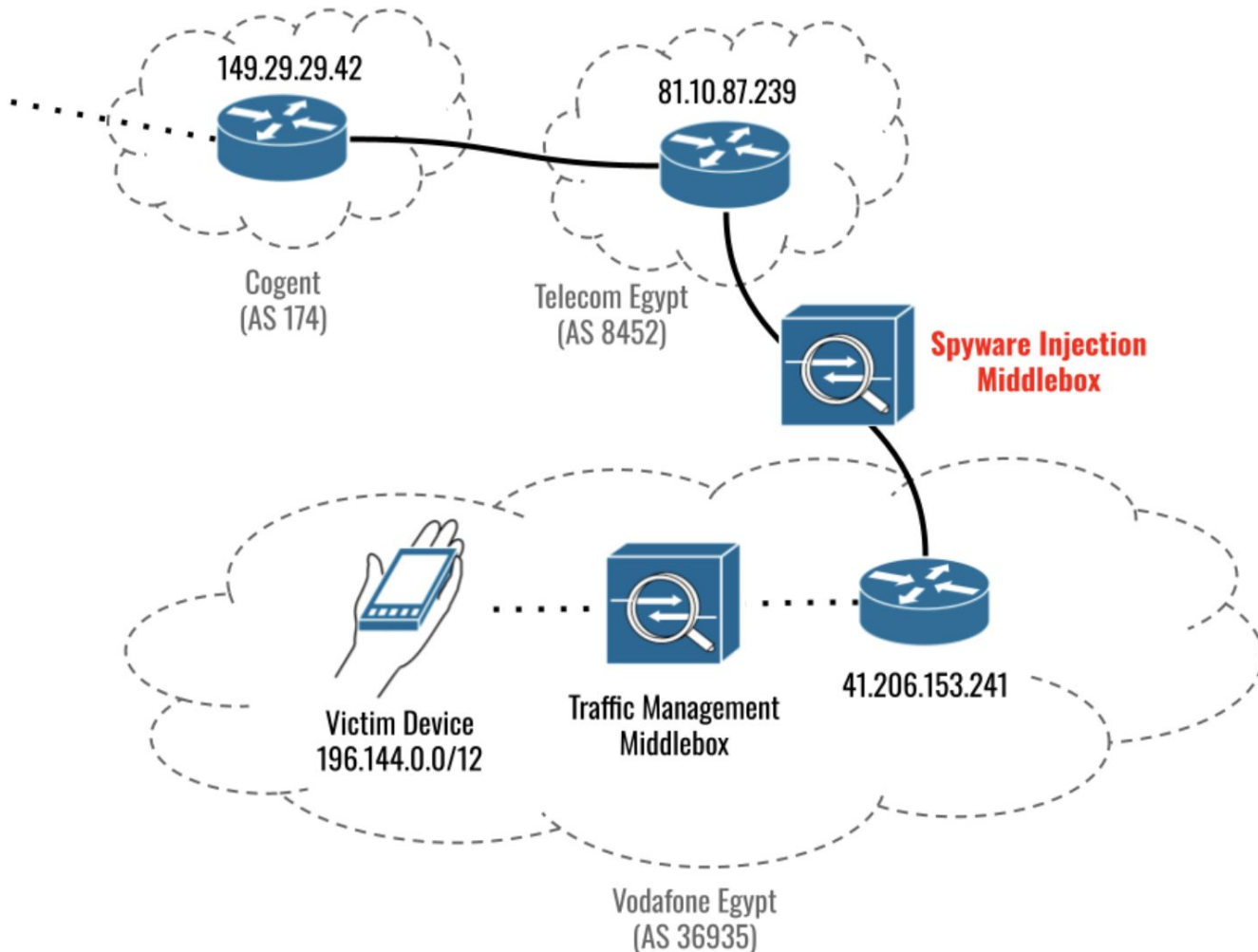


HTTP/1.
Via: 1.
Locatio
Connect

CVE-20
may lead

CVE-20
able to e

CVE-20
able to b



So, you've got a nation-wide MiTM capability?

So, you've got a nation-wide MiTM capability?



HTTP-01 challenge

This is the most common challenge type today. Let's Encrypt gives a token to your ACME client, and your ACME client puts a file on your web server at `http://<YOUR_DOMAIN>/.well-known/acme-challenge/<TOKEN>`.

So, you've got a nation-wide MiTM capability?



HTTP-01 challenge

This is the most common challenge type today. Let's Encrypt gives a token to your ACME client, and your ACME client puts a file on your web server at `http://<YOUR_DOMAIN>.well-known/acme-challenge/<TOKEN>`.

Infection techniques are evolving...

Revealed: Israeli Cyber Firms Have Developed an 'Insane' New Spyware Tool. No Defense Exists

A Haaretz investigation reveals that Israeli cyber companies developed technology that exploits the advertising system at the heart of the online economy to monitor civilians, hack into their phones and computers, and spy on them. This terrifying capability, against which no defense currently exists, has already been sold to a nondemocratic country



Zen Read

Infection techniques are evolving...

NSO Zero-Click Exploit: Turing-Complete CPU in Image File



by Richi Jennings on December 17, 2021

Press Release:

New document compression standard quadruples compression of today's fax standards and runs at unprecedented speeds

Infection techniques are evolving...

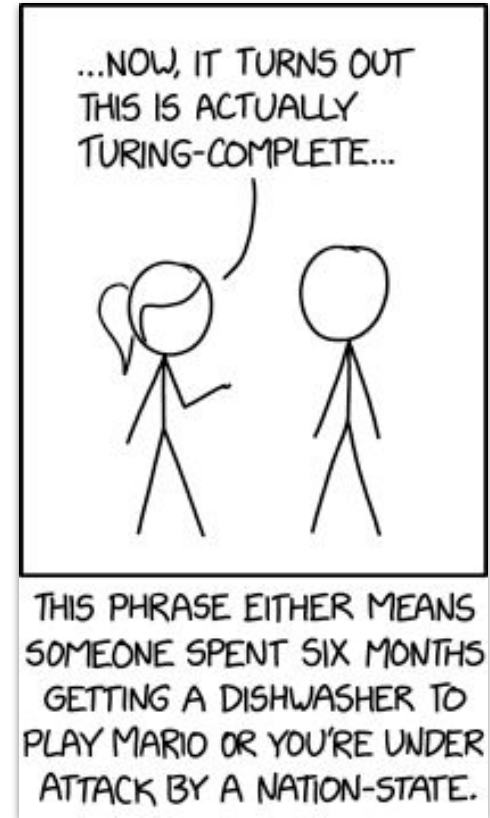
NSO Zero-Click Exploit: Turing-Complete CPU in Image File



by Richi Jennings on December 17, 2021

Press Release:

New document compression standard quadruples compression of today's fax standards and runs at unprecedented speeds



Infection techniques are evolving...



Infection techniques are evolving...



Google's OSS-Fuzz project has fuzzed hundreds of open source libraries for many years now, including libwebp

The problem, we now know, is that this format is incredibly complex and fragile, and the preconditions to trigger this issue are immense.

**What is "Mercenary
Spyware"?**

**How do targets get
hacked in practice?**

**Wait... how do we know
all this?**

Pivoting/Internet Scanning

Pivoting/Internet Scanning



If you've seen one **C&C server**, you've
seen them all.

— *Ronald Reagan* —

AZ QUOTES



HEY BILL...

**I THINK I'M BEING
TARGETED AGAIN...**

**Ahmed Mansoor
UAE Human Rights Activist**



**"NEW SECRETS ABOUT
TORTURE OF EMIRATIS IN
STATE PRISONS!"**

"If you've seen one, you've seen them all"



One

```
<html><head><meta http-equiv='refresh'  
content='0;url=http://www.google.com' /><m  
eta http-equiv='refresh'  
content='1;url=http://www.google.com' /><t  
itle></title></head><body></body></html>
```

"Them All"

"If you've seen one, you've seen them all"





Fingerprint #2
(273 IPs)



Ahmed Mansoor

2016



Fingerprint #1
(160 IPs)



Fingerprint #2
(273 IPs)

**41
IPs**



Ahmed Mansoor

2013-2015

2016



Fingerprint #1
(160 IPs)



nsoqa.com
qaintqa.com
mail1.nsoqgroup.com

2013-2015



Fingerprint #2
(273 IPs)



Ahmed Mansoor

2016

**41
IPs**



*WE FINGERPRINTED NSO GROUP SERVERS
BASED ON DISTINCTIVE RESPONSES!!*

(2016)



*WE FINGERPRINTED NSO GROUP SERVERS
BASED ON DISTINCTIVE RESPONSES!!*

(2016)

```
<html><head><meta http-equiv='refresh'  
content='0;url=http://www.google.com' />  
<meta http-equiv='refresh'  
content='1;url=http://www.google.com' />  
<title></title></head><body></body></html>
```

"Them All"



**WE FINGERPRINTED NSO GROUP SERVERS
BASED ON DISTINCTIVE RESPONSES!!**

(2016)

(2016-2018)

**LET'S SEE YOU FINGERPRINT A SERVER
THAT RETURNS A BLANK RESPONSE!!**





**WE FINGERPRINTED NSO GROUP SERVERS
BASED ON DISTINCTIVE RESPONSES!!**

(2016)

(2016-2018)

**LET'S SEE YOU FINGERPRINT A SERVER
THAT RETURNS A BLANK RESPONSE!!**



**OK, BUT WE CAN STILL FINGERPRINT BASED
ON THE TLS HANDSHAKE!!**

(2018)



Fingerprint #1
(160 IPs)



nsoqa.com
qaintqa.com
mail1.nsoqgroup.com

2013-2015



Fingerprint #2
(273 IPs)



Ahmed Mansoor

2016



Fingerprint #3
(1149 IPs)

41
IPs

1
IP,
7
Doms,*
2
Certs

2016-2018



**WE FINGERPRINTED NSO GROUP SERVERS
BASED ON DISTINCTIVE RESPONSES!!**

(2016)

(2016-2018)

**LET'S SEE YOU FINGERPRINT A SERVER
THAT RETURNS A BLANK RESPONSE!!**



**OK, BUT WE CAN STILL FINGERPRINT BASED
ON THE TLS HANDSHAKE!!**

(2018)

(2018-2020)

**NOT IF THE SERVER USES PORT
KNOCKING AND HAS NO OPEN PORTS!!**





**WE FINGERPRINTED NSO GROUP SERVERS
BASED ON DISTINCTIVE RESPONSES!!**

(2016)

(2016-2018)

**LET'S SEE YOU FINGERPRINT A SERVER
THAT RETURNS A BLANK RESPONSE!!**



**OK, BUT WE CAN STILL FINGERPRINT BASED
ON THE TLS HANDSHAKE!!**

(2018)

(2018-2020)

**NOT IF THE SERVER USES PORT
KNOCKING AND HAS NO OPEN PORTS!!**



WELL ACTUALLY...

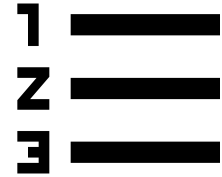
(2020)

Log Analysis

Log Analysis

Top-Down:

Analyze a spyware sample, understand what traces it leaves behind, then look for these traces



Log Analysis

Top-Down:

Analyze a spyware sample, understand what traces it leaves behind, then look for these traces



Bottom-Up:

Analyze phone logs, looking for *implausible artifacts*, then analyze to see if these are traces of spyware



Log Analysis

Top-Down:

Analyze a spyware sample, understand what traces it leaves behind, then look for these traces



Bottom-Up:

Analyze phone logs, looking for *implausible artifacts*, then analyze to see if these are traces of spyware



(CAN DETECT HERETOFORE UNKNOWN SPYWARE THIS WAY!!)

What is "Mercenary
Spyware"?

How do targets get
hacked in practice?

Wait... how do we know
all this?

Surely this is "just a
technical problem"?

Burn the exploits!

NSO Zero-Click Exploit: Turing-Complete CPU in Image File



by Richi Jennings on December 17, 2021

Burn the exploits!

NSO Zero-Click Exploit: Turing-Complete CPU in Image File



by Richi Jennings on December 17, 2021

CVE-2021-30860: Processing a maliciously crafted PDF may lead to arbitrary code execution.

CVE-2021-31010: A deserialization issue was addressed through improved validation



So did that work?

So did that work?

- Jan 2022: **LATENTIMAGE** (*Find My*)



So did that work?

- Jan 2022: **LATENTIMAGE** (*Find My*)
- Jun 2022: **FINDMYPWN** (*Find My + BlastDoor*)



So did that work?

- Jan 2022: **LATENTIMAGE** (*Find My*)
- Jun 2022: **FINDMYPWN** (*Find My + BlastDoor*)
- Oct 2022: **PWNYOURHOME** (*HomeKit + BlastDoor*)



So did that work?

- Jan 2022: **LATENTIMAGE** (*Find My*)
- Jun 2022: **FINDMYPWN** (*Find My + BlastDoor*)
- Oct 2022: **PWNYOURHOME** (*HomeKit + BlastDoor*)
- Sep 2023: **BLASTPASS** (*HomeKit + WebP + BlastDoor SBX*)
 - We got (part of) this one! **CVE-2023-41064**



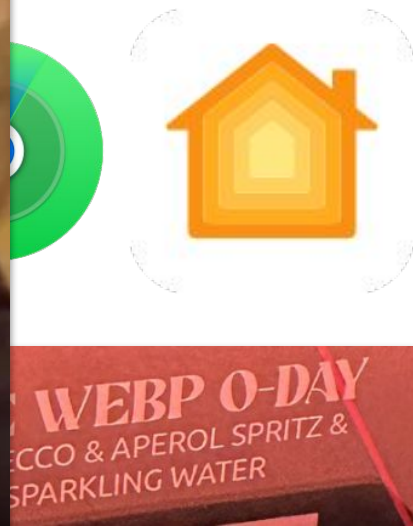
So did that work? **Nope.**

- Jan 2022: **LATENTIMAGE** (*Find My*)
- Jun 2022: **FINDMYPWN** (*Find My + BlastDoor*)
- Oct 2022: **PWNYOURHOME** (*HomeKit + BlastDoor*)
- Sep 2023: **BLASTPASS** (*HomeKit + WebP + BlastDoor SBX*)
 - We got (part of) this one! **CVE-2023-41064**
- etc, etc.



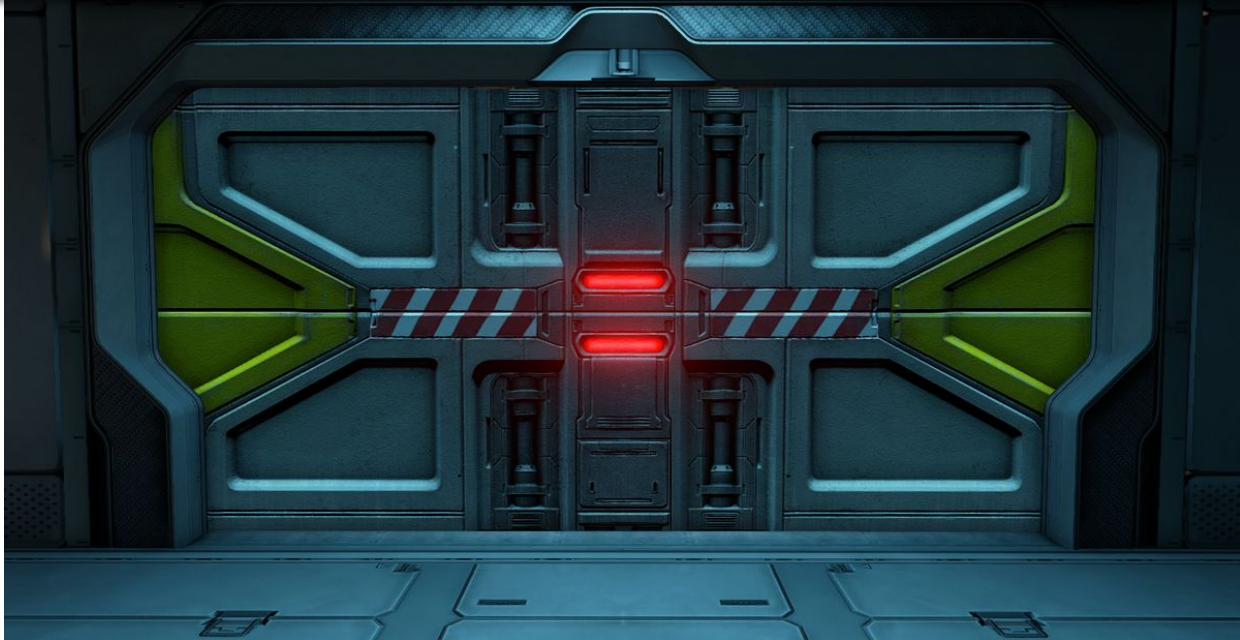
So did that work? **Nope.**

- Jan 2022: **LATENTIMAGE**
 - Jun 2022: **FINDMYPWN** (
 - Oct 2022: **PWNYOURHO**
 - Sep 2023: **BLASTPASS** (
 - We got (part of)
- etc, etc.

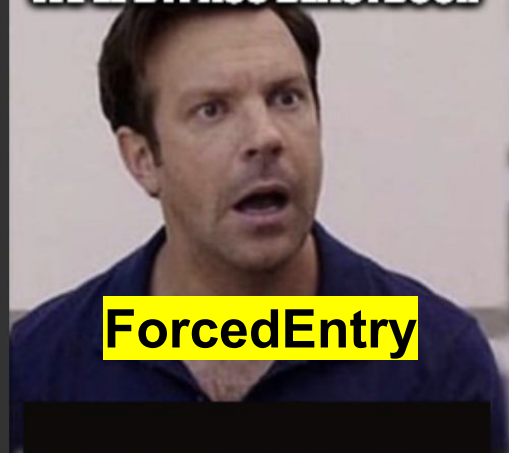


What about new mitigations?

Apple iOS 14 Thwarts iMessage Attacks With BlastDoor System



WE'LL BYPASS BLASTDOOR



ForcedEntry

WE'LL BYPASS BLASTDOOR



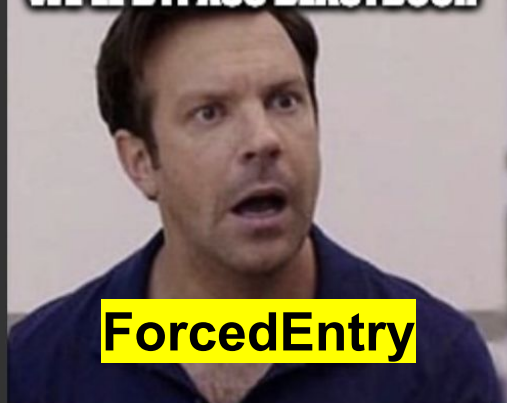
ForcedEntry

**WE'LL BREAK OUT OF
THE BLASTDOOR SANDBOX**



BlastPass

WE'LL BYPASS BLASTDOOR



ForcedEntry

**WE'LL BREAK OUT OF
THE BLASTDOOR SANDBOX**



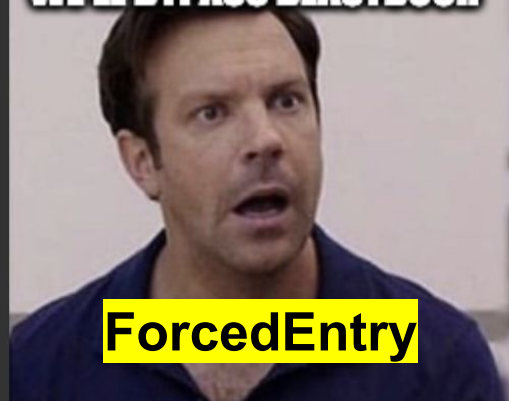
BlastPass

EndOfDays



**WE'LL ATTACK
ICALNDAR INSTEAD**

WE'LL BYPASS BLASTDOOR



ForcedEntry

**WE'LL BREAK OUT OF
THE BLASTDOOR SANDBOX**



BlastPass

EndOfDays



**WE'LL ATTACK
ICALENDAR INSTEAD**

Triangulation



**YOU GUYS ARE
WORRYING ABOUT BLASTDOOR?**

What about new(er) mitigations?



Friday, September 9

9:41

Notification Center



Lockdown Mode block... Yesterday

[redacted]@gmail.com attempted to access a Home.



Lockdown Mode block... Mon

[redacted]@yahoo.com attempted to access a Home.

 **Elon Musk**   @elonmusk · Jun 1 ...

Does lockdown mode address this?



 107  62  697  80.8K 

 **Eugene Kaspersky**   @e_kaspersky ...

Yes, we do recommend disabling iMessage and enable the lockdown mode

2:10 AM · Jun 2, 2023 · **1,941** Views

2 Retweets **29** Likes

  **Lockdown Mode block...** Mon

[redacted]@yahoo.com attempted to access a Home.

 **Elon Musk**   @elonmusk · Jun 1


Does lockdown mode address this?

 107  62  697  80.8K 

OK THIS ONE ACTUALLY HAS AN IMPACT!

2:10 AM · Jun 2, 2023 · **1,941** Views

2 Retweets **29** Likes

 **Lockdown Mode block...** Mon

[redacted]@yahoo.com attempted to access a Home.



Elon Musk   @elonmusk · Jun 1


Does lockdown mode address this?

 107  62  697  80.8K 

BUT...

2:10 AM · Jun 2, 2023 · 1,941 Views

2 Retweets 29 Likes



Lockdown Mode block... Mon

[redacted]@yahoo.com attempted to access a Home.

What about new(er) mitigations?



What about notifications?



Threat Notification

November 23, 2021

Apple sent the following threat notification via email to [REDACTED] and via iMessage to [REDACTED]. We also sent a short notification to the recovery contacts associated with your account.

ALERT: State-sponsored attackers may be targeting your iPhone

What about notifications?



Threat Notification

November 23, 2021

Apple sent the following threat notification via email to [REDACTED] and via iMessage to [REDACTED]. We also sent a short notification to the recovery contacts associated with your account.

ALERT: State-sponsored attackers may be targeting your iPhone

150 COUNTRIES!!

What about notifications?



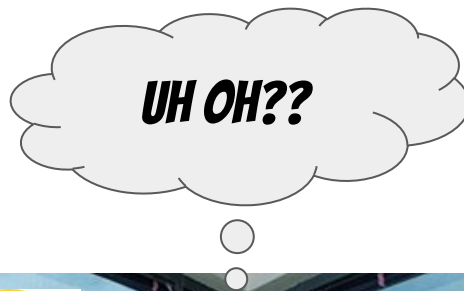
Threat Notification

November 23, 2021

Apple sent the following threat notification via email to [REDACTED] and via iMessage to [REDACTED]. We also sent a short notification to the recovery contacts associated with your account.

ALERT: State-sponsored attackers may be targeting your iPhone

150 COUNTRIES!!



Do threat actors care about notifications?

Apple Threat Notifications:

- Nov 2021
- Nov 2022
- Dec 2022
- Mar 2023
- Jun 2023
- Oct 2023

Do threat actors care about notifications?

Apple Threat Notifications:

- Nov 2021
- Nov 2022
- Dec 2022
- Mar 2023
- Jun 2023
- Oct 2023

Threat Actors:



Indian opposition MPs accuse government of trying to hack their iPhones

At least eight prominent Indian opposition politicians have reported receiving warnings from Apple that “state-sponsored attackers” might have targeted their iPhones, raising concerns about possible digital espionage ahead of next year’s general election.

Indian opposition MPs accuse government of trying to hack their iPhones

At least eight prominent Indian opposition politicians have reported receiving warnings from Apple that “state-sponsored attackers” might have targeted their iPhones, raising concerns about possible digital espionage ahead of next year’s general election.

Govt investigating whether China-linked agencies are behind Apple spyware attack

Indian opposition MPs accuse govt of trying to hack their iPhones

***IT COULD BE SOMEONE
SITTING ON THEIR BED THAT
WEIGHS 400 POUNDS***



espionage ahead of next

**r China-
Apple**

spyware attack

At
wa
the
yea

Things could be better if...

- Mitigations move from optional → mandatory (e.g., Lockdown Mode takes the "2FA path")
- Better specificity from tech companies on threats
- For high-risk users, complex devices will *eventually* be hacked; design accordingly

There's also a role for... (gasp)... regulation



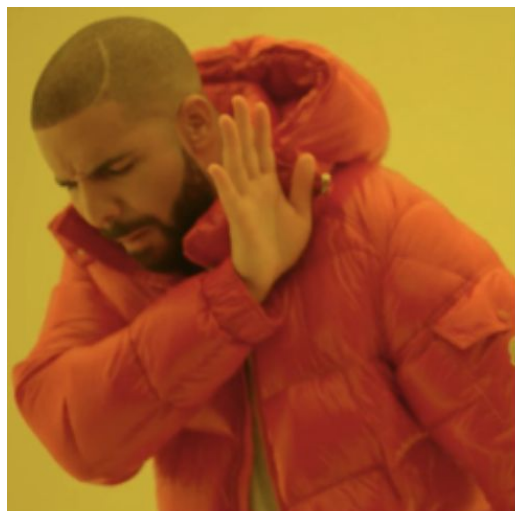
SECURITY RESEARCHERS SAY a proposed set of export rules meant to restrict the sale of surveillance software to repressive regimes are so broadly written that they could criminalize some research and restrict legitimate tools that professionals need to make software and computer systems more secure.



SECURITY RESEARCHERS SAY a proposed set of export rules meant to restrict the sale of surveillance software to repressive regimes are so broadly written that they could criminalize some research and restrict legitimate tools that professionals need to make software and computer systems more secure.

Hacking Team loses global license to sell spyware

The move coincides with a sharp rise in diplomatic tensions between Italy and Egypt over the brutal murder of Giulio Regeni, a 28-year old Italian researcher in Cairo.



**Regulating
technologies**



**Regulating
companies**

NSO Pegasus spyware can no longer target UK phone numbers

Israeli maker of surveillance software blocked +44 code after detecting hack against Princess Haya, source says

“We shut down completely, hard-coded into the system [Pegasus], to all of our customers. We released a quick update in the middle of the night that none of our customers can work on UK numbers,” the source close to the company added.

forbidden stories

🔒 PROTECT YOUR STORIES



THE PEGASUS PROJECT

LIRE EN FRANÇAIS

forbidden stories

🔒 PROTECT YOUR STORIES



PROJECT

LIRE EN FRANÇAIS

Scoop: Israel and France hold secret talks to end NSO spyware crisis

- The Israeli proposal included a **commitment to ban the hacking of French mobile phone numbers** in any future spyware deal between an Israeli firm and a third country.
- A similar ban already exists on hacking U.S. and U.K. numbers.

US State Department phones were reportedly hacked by NSO spyware

At least nine employees of the US State Department working in or with Uganda had their iPhones hacked with spyware made by NSO Group,

US State Department phones were reportedly hacked by NSO spyware

At least nine employees of the US State Department working in or with Uganda had their iPhones hacked with spyware made by NSO Group,

**Commerce Adds NSO Group
and Other Foreign Companies
to Entity List for Malicious
Cyber Activities**

US State Department phones were reportedly hacked by NSO spyware

At least nine employees of the US State Department working in or with Uganda had their iPhones hacked with spyware made by NSO Group,

Commerce Adds NSO Group
companies. Wednesday's move sanctions specific companies but sweeps broadly on the technology and items covered. American-made toilet paper, for instance, would be barred from being sent to NSO Group or any of the other listed companies.

CYBER ACTIVITIES

Vietnam tried to hack U.S. officials, CNN with posts on X, probe finds

The attempts appear to have been unsuccessful, but came as the U.S. and Vietnam were negotiating an agreement that President Biden signed last month in Hanoi

Vietnam tri with posts o

The attempts appear to
were negotiating an ag

cial, CNN

is the U.S. and Vietnam
last month in Hanoi



Etilda Gjonaj @GjonajEtilda · May 23

Honored to discuss with 🇺🇸 Senators @ChrisMurphyCT & @GaryPeters on European integration of Albania, rule of law and justice reform! 🇷🇺 🇪🇺



Ambassador Yuri Kim 🇺🇸 @USAmbAlbania · May 23

1/2 Great to have Senators @ChrisMurphyCT and @GaryPeters in Albania to strengthen 🇺🇸 🇷🇺 relations across democracy, defense, and business. As Sen. Murphy said, "The U.S. has no better friend in the world than Albania."

[Show this thread](#)



1



1



6



434



Joseph Gordon

@Joseph_Gordon16

Replying to @GjonajEtilda @ChrisMurphyCT and @GaryPeters

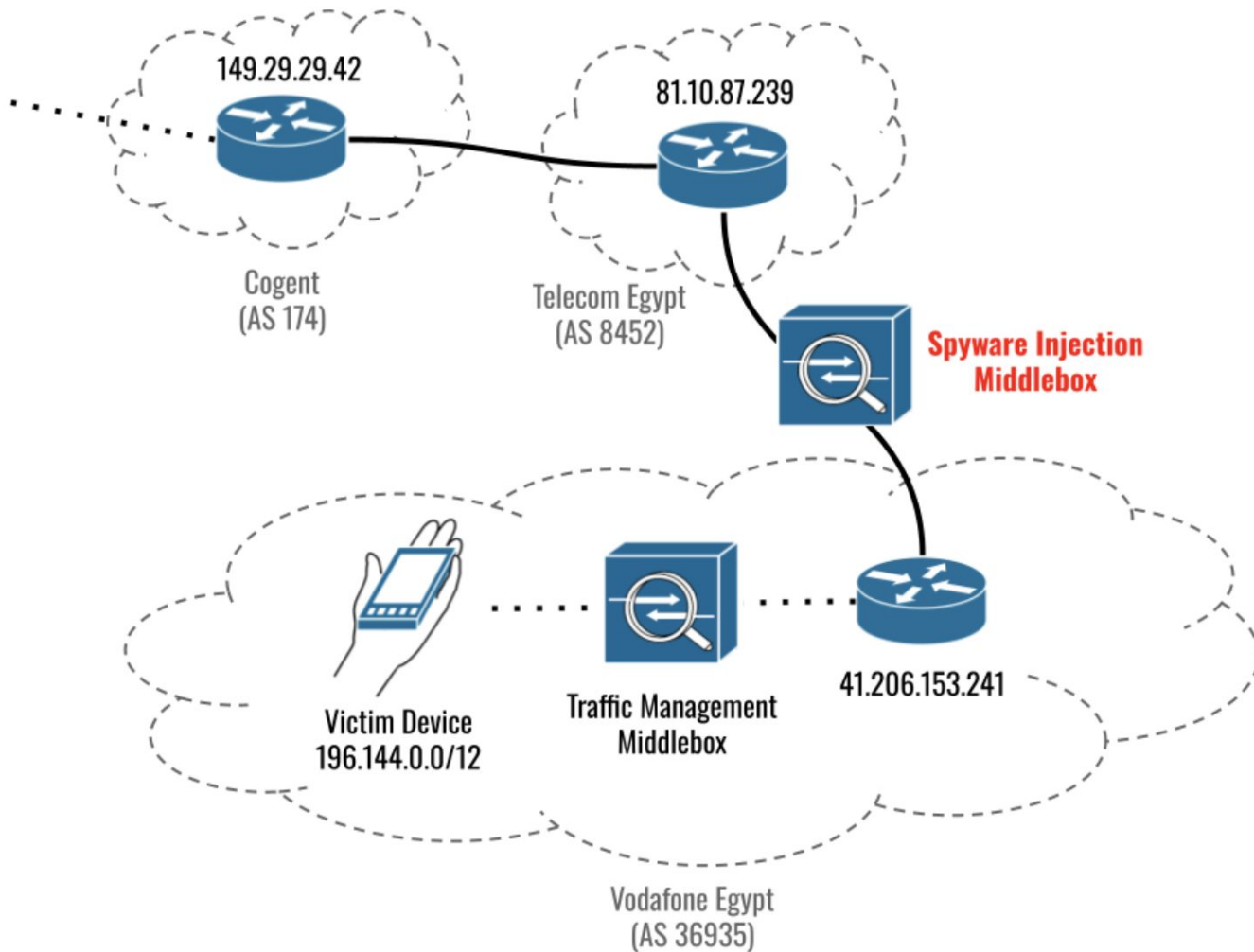
UK aims to deter Albanian refugees with 'make clear the perils' ad campaign southchinapost.net/enISDKnl

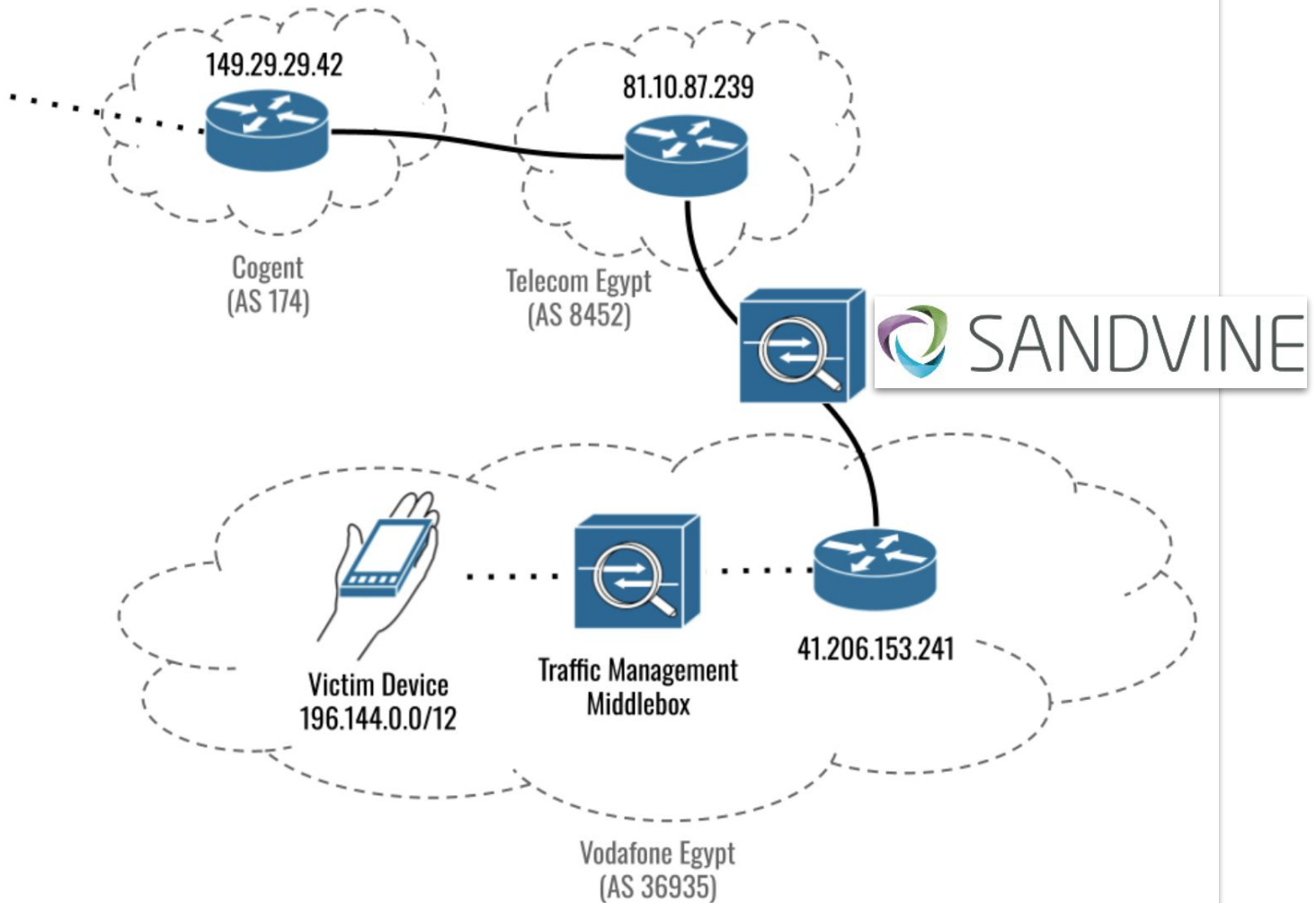
4:35 AM · Jun 1, 2023 · 2 Views

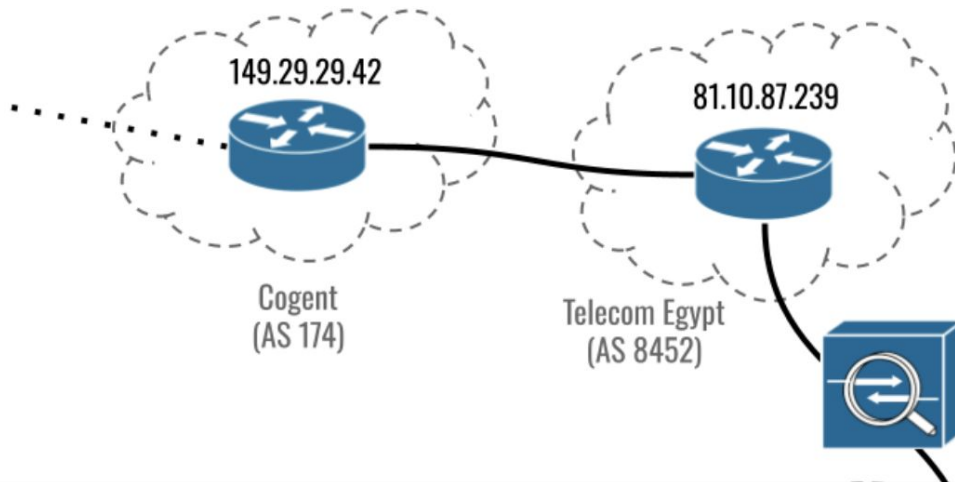


I WANT YOU

To stop doing business with NSO
Group, Intellexa, Cytrox, Candiru





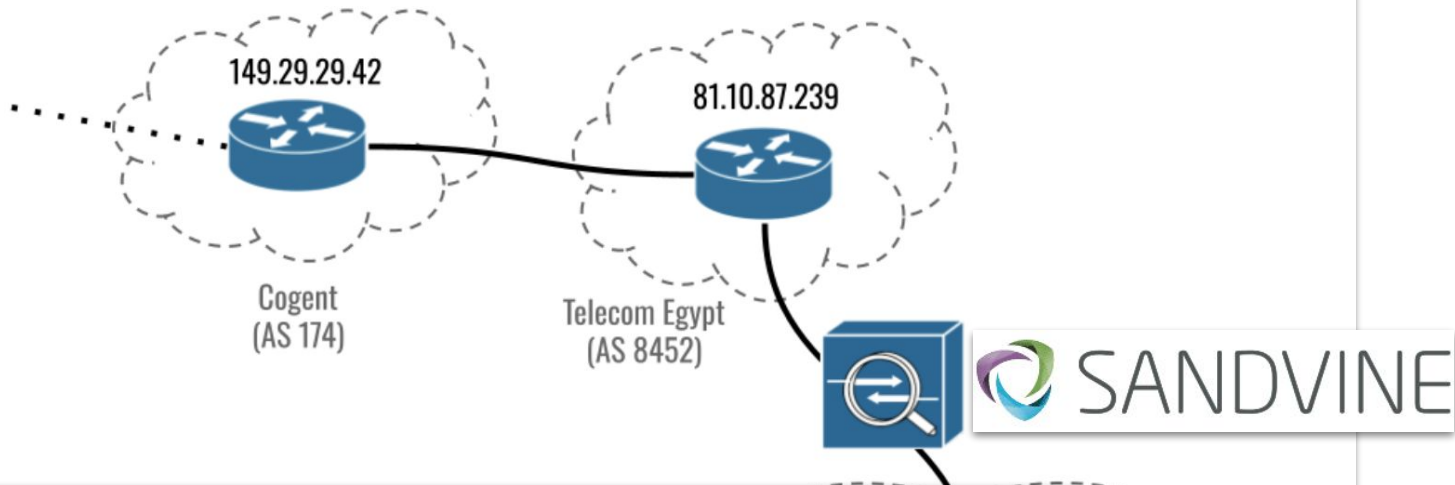



 **The Register**  

CSO **11** 

Sandvine put on America's export no-fly list after Egypt used network tech for spying

Vodafone Egypt (AS 36935)



CSO **11** 

**Sandvine put
after Egypt us**

Rating Action
**Moody's downgrades Sandvine's CFR to Caa1;
outlook remains negative**



ALL YOUR PLAINTEXT ARE BELONG TO US