The Million Dollar Dissident

EMS 8803 Discussion

By Chaitanya Rahalkar & Nathan Jaco

Georgia Tech College of Computing
School of Cybersecurity and Privacy

Presentation Structure

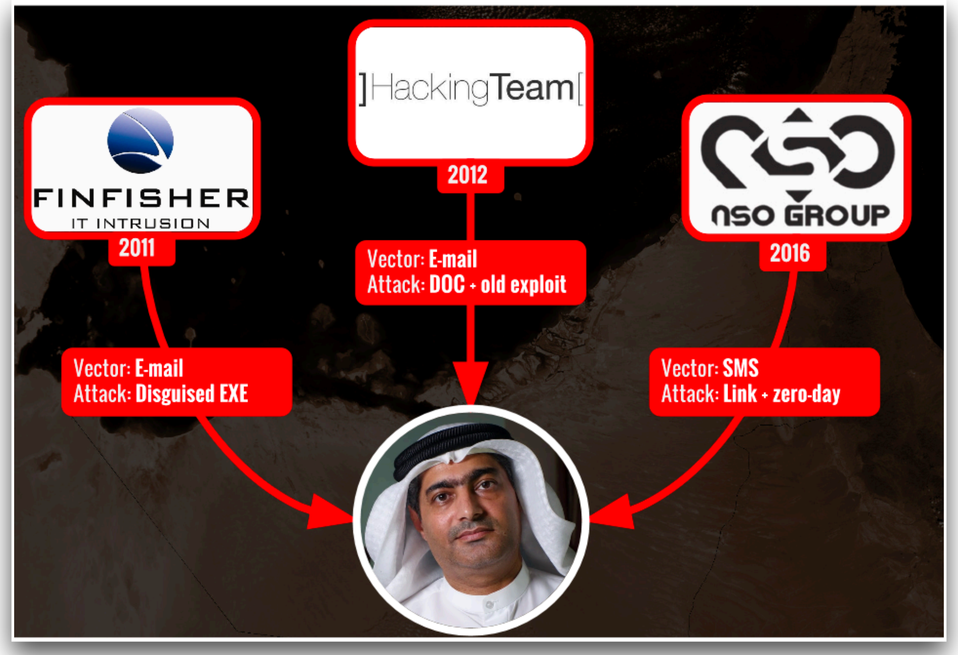
1. Background
2. Overview of the Attack
3. Discovery of Attack Infrastructure
4. Post-mortem Analysis
5. Conclusion

Background: Protecting Civil Society from State Surveillance

- Information and Communications Technology has changed (whether improved by it is questionable) the lives of much of the world's population.
- Access to (mis)information has exponentially increased.
- Never have authoritarian regimes possessed greater power to surveil civil society.
- Never have liberal capitalist democratic regimes possessed greater power to develop and monetize tools for authoritarian regimes to surveil civil society.

Background: The Asset Profile - Ahmed Mansoor

- Ahmed Mansoor in a well-known human rights advocate in the United Arab Emirates.
- He is a Martin Ennals awardee and is a prime candidate for targeting by Spyware.
- Unsurprisingly for a man in his position, he turns out to have some reasonable amount of cybersecurity sophistication.
- Mansoor had been previously targeted with multiple attacks, including the FinFisher Trojan horse, a complex piece of government-surveillance malware that is peskily persistent on infected machines.



Background: The Organizational Profile - Citizen Lab

- Citizen Lab is an interdisciplinary technology/policy lab out of the UT Munk School.

- Citizen Lab's work helps protect civil society activists and advocates from cyber threats.

- Inter alia, Citizen Lab is engaged in -
  - Investigating digital espionage against civil society.
  - Documenting Internet filtering and other technologies and practices that impact freedom of expression online.
  - Analyzing privacy, security, and information controls of popular applications.

Background: The Target Profile - NSO Group

- The NSO Group is a software provider and cyber warfare company. It was founded by probable veterans of Israeli Defense Forces SIGINT Unit 8200.
- NSO Group maintains partnerships in the ecosystem of Israeli private espionage. Its products are highly valued by governments. Pegasus is their well known offering.
- NSO Group is believed to have provided spyware to several problematic entities including corrupt politicians in Panama and Mexico, as well as the UAE.
- The NSO Group found itself under FBI investigation and questions swirled about whether it was a supplier to the Saudis.
- Pegasus was found on the phone of close associates of slain journalist Jamal Khashoggi.

Overview of the Attack

Link is a part of NSO's exploit infrastructure

SMS Received on Mansoor's iPhone 6 running iOS 9.3.3
Translation: "New secrets about torture of Emiratis in state prisons"

Overview of the Attack (con't)

The Trident Exploit Chain

- Trident is a collection of zero-day vulnerabilities that allowed for an advanced and persistent mobile security attack on iOS-mediated devices.
- The attack is initialized by a spear-phishing link.
- The attack had a sophisticated exploit chain with multiple zero-days (perhaps a hallmark of Israeli Cyber Ops such as Stuxnet).
- It enabled remote and surreptitious jailbreaking of an iOS mobile device for data exfiltration.

Overview of the Attack (con't)

The Trident Exploit Chain

- CVE-2016-4657: An exploit for WebKit, which allows execution of the initial shellcode. Staged exploit that allowed execution of code within the context of the browser.

- CVE-2016-4655: A Kernel Address Space Layout Randomization (KASLR) bypass exploit to find the base address of the kernel.

- CVE-2016-4656: 32 and 64 bit iOS kernel exploits that allow execution of code in the kernel, used to jailbreak the phone and allow software installation. Disables code signing enforcement, allowing the running of unsigned binaries (the Pegasus spyware)

- Three exploits chained together to achieve complete control.

Overview of the Attack (con't)

The Trident Exploit Chain

- CVE-2016-4657: An exploit for WebKit, which allows execution of the initial shellcode. Staged exploit that allowed execution of code within the context of the browser.

- CVE-2016-4655: A Kernel Address Space Layout Randomization (KASLR) bypass exploit to find the base address of the kernel.

- CVE-2016-4656: 32 and 64 bit iOS kernel exploits that allow execution of code in the kernel, used to jailbreak the phone and allow software installation. Disables code signing enforcement, allowing the running of unsigned binaries (the Pegasus spyware)

- Three exploits chained together to achieve complete control.

Overview of the Attack (con't)

The Payload

```
GET /[redacted]/ HTTP/1.1
HTTP/1.1 200 OK  (text/html)
GET /[redacted]/ntf_xps.html&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=1&nocache=[redacted] HTTP/1.1
GET /[redacted]//final111?&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=2&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=[redacted]&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK  (application/octet-stream)
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=3&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
HTTP/1.1 200 OK
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=4&nocache=[redacted] HTTP/1.1
GET /[redacted]/ntf_xpe.html&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
HTTP/1.1 200 OK
GET /[redacted]/ntf_bed.html?s=[redacted]&d= HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_brc.html?m=0 HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_bed.html?s=[redacted]&d=Tring%20to%20download%20bundle%28try%3A0%29 HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/test111.tar HTTP/1.1
```

Intermediate Files

Final Payload

Overview of the Attack (con't)

The Payload - Uncovered

- **Persistence** - The payload re-runs every time the phone is rebooted using the JavascriptCore binary. It disables Apple's automatic updates, detects and removes jailbreaks.
- **Recording** - Used renamed copy of Cydia substrate, a third-party app developer framework to record calls. It had the ability to spy on apps like: iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, Skype, WeChat and many more
- **Exfiltration** - Payload sends Base64 encoded beacons to the C&C server.

```
Your Google verification code is:5678429
http://gmail.com/?
z=FEcCAA==&i=MTphYWxhYW4udHY6NDQzLDE6bWFub3Jhb25saW5lLm5ldDo0NDM=&s=zpvzPSYS674=
```

Base 64 Decoded Beacon

```
1:aalaan.tv:443,1:manoraonline.net:443
```

C&C Servers in "I" parameter of URL

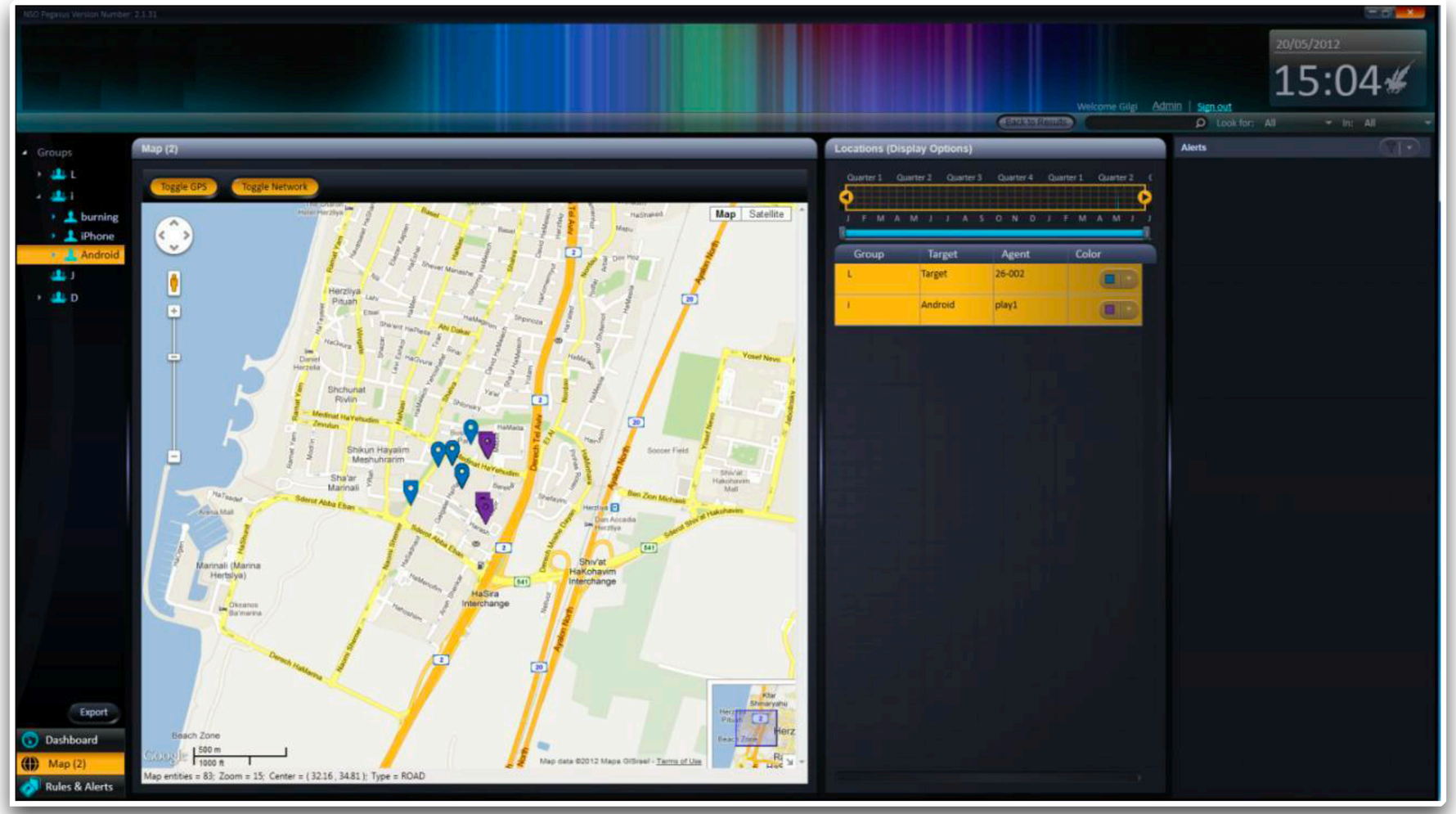
Overview of the Attack (con't)

Impact of the Implant

- A successful implant of any NSO spyware (like Pegasus) could typically retrieve photos, recordings, messages, files, call logs, browsing history, WhatsApp calls & messages, emails etc.
- All data was sent back to a Pegasus Data Server via a custom built proxy system called PATN (Pegasus Anonymizing Transmission Network) to obfuscate the identity of the client associated with the operation.
- Mansoor's implant communicated with two PATN nodes - aalaan.tv and manoraonline.net.

Overview of the Attack (con't)

Pegasus Working Station Software



Source: Hacking Team Data Breach of Emails

Discovery of Attack Infrastructure

Hints of Pegasus in the Payload

```
_kPegasusProtocolAgentControlElement_iv
_kPegasusProtocolAgentControlElement_key
_kPegasusProtocolAgentControlElement_ciphertext
_kPegasusProtocolProtocolElement_iv
_kPegasusProtocolProtocolElement_key
_kPegasusProtocolProtocolElement_ciphertext
_kPegasusProtocolResponseElement_iv
_kPegasusProtocolResponseElement_key
_kPegasusProtocolResponseElement_ciphertext
```

Pegasus String in the Payload - test111.tar

Payload contained several dynamically linked libraries - libaudio.dylib, libimo.dylib libwacalls.dylib (WhatsApp), libvb.dylib (Viber).

Discovery of Attack Infrastructure

Stealth Falcon Leads to Discovery

- Prior to this, Citizen Lab was tracking Stealth Falcon's spyware. A discovered domain - smser.net had several fingerprints on Shodan, Censys and their own scanning investigation with ZMap.
- 237 live IP addresses were found and domain names were extracted from SSL certificates used by these IPs. The domains - *.webadv.co, aalaan.tv and manoraonline.net were discovered in few of the SSL certificates which were found in the spyware attack sent to Mansoor.
- They further coded the domains found and categorized them as per their theme.

Discovery of Attack Infrastructure

Categorization of Discovered Domains

Type	Example	Impersonating
News Media	alljazeera.co bbc-africa.com cnn-africa.co unonoticias.net univision.click	Aljazeera BBC CNN Las Ultimas Noticias Univision
Shipment Tracking	track-your-fedex-package.org	FedEx
ISP / Telco	mz-vodacom.info iusacell-movil. com.mx sabafon.info newtarrifs.net	Vodacom (Mozambique) Iusacell (Mexico) Sabafon (Yemen) Generic
Popular Online Platforms	y0utube.com.mx fb-accounts.com googleplay-store.com whatsapp-app.com	YouTube Facebook Google WhatsApp
Account Info. (Generic)	accounts.mx adjust-local-settings.com	Unknown
Government Portals	emiratesfoundation.net topcontactco.com	The Emirates Foundation Teleperformance Visa Application Processing Portal for the UK (tpcontact.co.uk.)

Discovery of Attack Infrastructure

Linking Historical Data to Attack on Mansoor

- The link sent to Mansoor used the domain sms.webadv.co. A wildcard SSL certificate for webadv.co was found in previous discovery.
- The list of IPs also included IPs for the two C2 servers aalaan.tv and manoraonline.tv. These IP addresses were found to be of cloud VPS providers.
- 19 IPs from the list resolved to manoraonline.tv at some point.
- From October 2013 to September 2014, 83 IPs from other historical data matched the fingerprint of manoraonline.tv
- Two IPs that matched the fingerprint had sometime previously pointed to mail1.nsogroup.com and nsoqa.com (domains registered by NSO).

Present Day

- Zero Day exploits continue to be used by NSO to perform surveillance.
- “ForcedEntry” - Zero Click exploit found in iMessage used to target yet another Saudi activist.
- Discovered and documented on Sept. 13, 2021 by CitizenLab.
- Patches for CVE-2021-30860 released immediately by Apple after revelation.
- Exploit affected not just iPhones, but also the Mac, iPad and Apple Watch.
- Maliciously crafted “.gif” had the exploit chain.

Present Day

Breaking the News

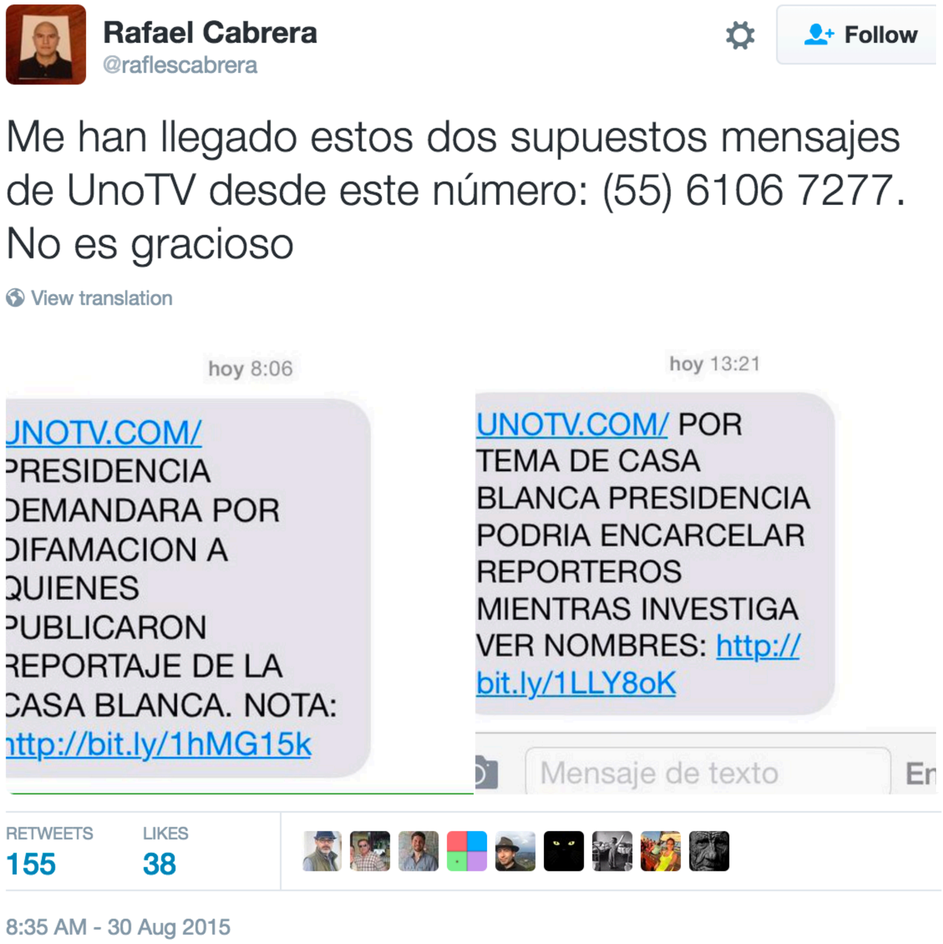
New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts

By Bill Marczak, John Scott-Railton, Siena Anstis, Bahr Abdul Razzak, and Ron Deibert

October 24, 2021

Ref. Citizen Lab Article

Evidence of Other Targets

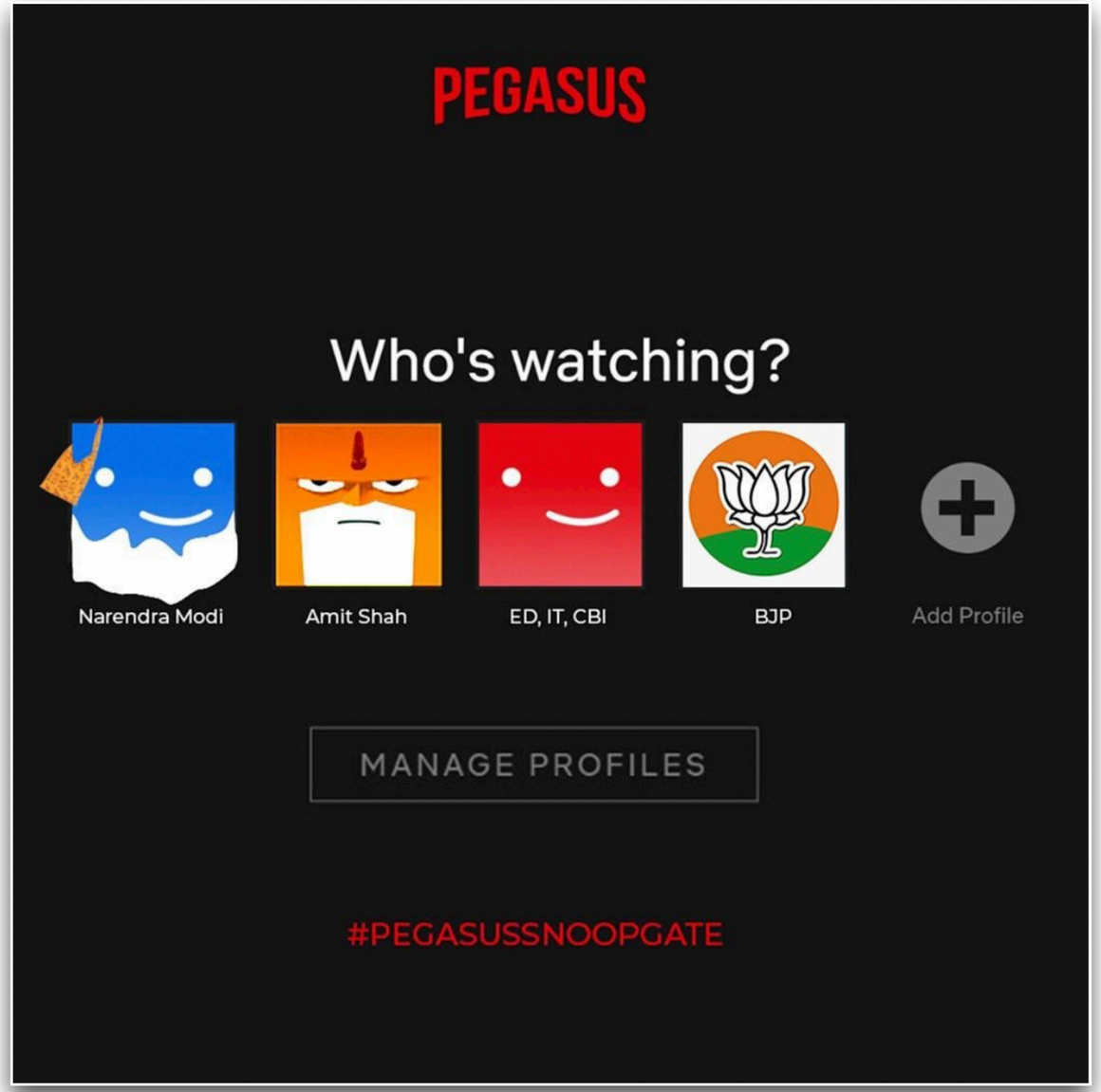


Translation: UNOTV.COM/ THE PRESIDENT'S OFFICE WILL SUE FOR DEFAMATION THOSE WHO PUBLISH REPORTING ON CASA BLANCA. NOTE: [MALICIOUS LINK]

Translation: UNOTV.COM/ ON THE TOPIC OF THE CASA BLANCA, THE PRESIDENCY COULD INCARCERATE REPORTERS WHILE THEY LOOK INTO THE

Kenya: A Tweet Discussing the Opposition

Evidence of Other Targets



Indian supreme court orders inquiry into state's use of Pegasus spyware

Judges criticise Modi government's refusal to divulge what software was used for and why

After Action Review: The Mansoor Affair

- The Citizen Lab report uncovered one of the most advanced mobile security threats to date.
- Said report led to Apple releasing an iOS patch.
- This is a success story of the responsible disclosure process.
- There exists a framework of economic incentives for developing dangerous software.
- Spyware tools are developed in liberal democracies and spread to the non-aligned world.
- Existing export controls are insufficient.

The State of Play

- International cyberspace is a disorderly environment.
- Every government is an authoritarian regime to its own political dissidents.
- It is important to shed light on this because governments have unprecedented powers of surveillance over civil society due to a nexus of public and private actors.
- It may perhaps be fair to characterize Israel as rogue state in the cyber arms trade.

Questions (con't)

- From FOSS and closed-source software development, which is more susceptible to zero day exploitation? Does the security design principle of "Open Design" really help?
- How can we better regulate the international cyber arms trade?
- How can we integrate technical and policy solutions to cyber weapons anti-proliferation?
- Do we need to include cyber weapons development and containment ethics into the cybersecurity education curriculum?
- Is the world too interconnected?

Questions (con’t)

- What are your thoughts on big tech companies neglecting security researchers’ efforts in responsibly disclosing bugs? From the standpoint of the security researcher - Was this the right thing to do?

Thank You!