CHECK POINT CloudGuard Dome9

Is your internet down? It’s cyber warfare, stupid!

Shira Shamban
CheckPoint

Who am I?

Shira

8200

Dome9 Security

CheckPoint

OWASP

History repeats itself

Technology changed spying and weapons.

Who’s in a cold war today?

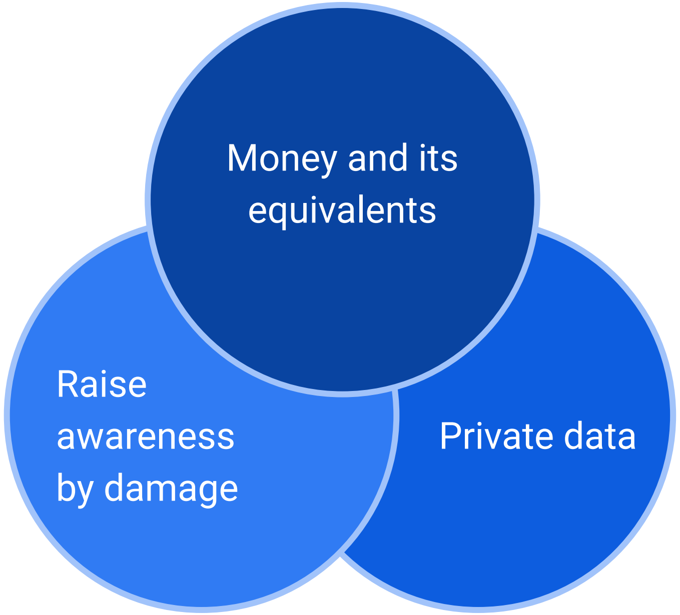
From dirty bombs to dirty warms.

This kind of warfare gives us new challenges:

- ➔ Detection - how can you tell you’ve been hacked?
- ➔ Damage and impact
- ➔ Preparation and defence
- ➔ Psychological effect
- ➔ Attribution

Criminal hacker vs. State hacker - what's the difference?

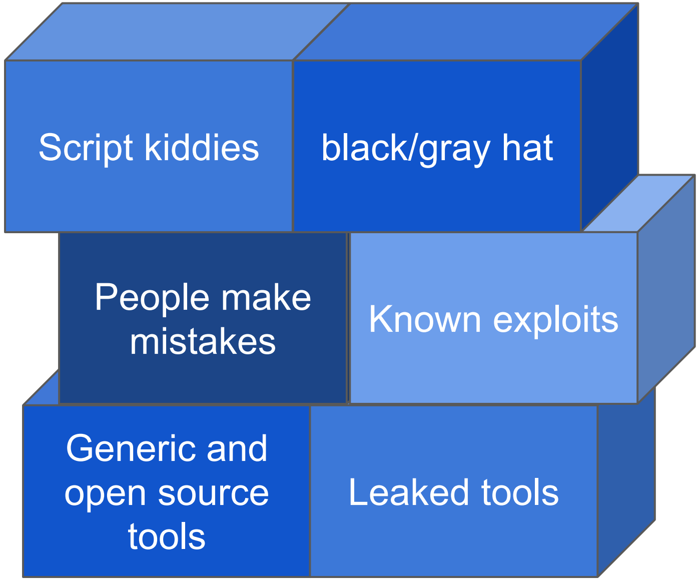
Goals



Detectable impact

No immediate impact
Might never get detected

Tools and resources



Script kiddies

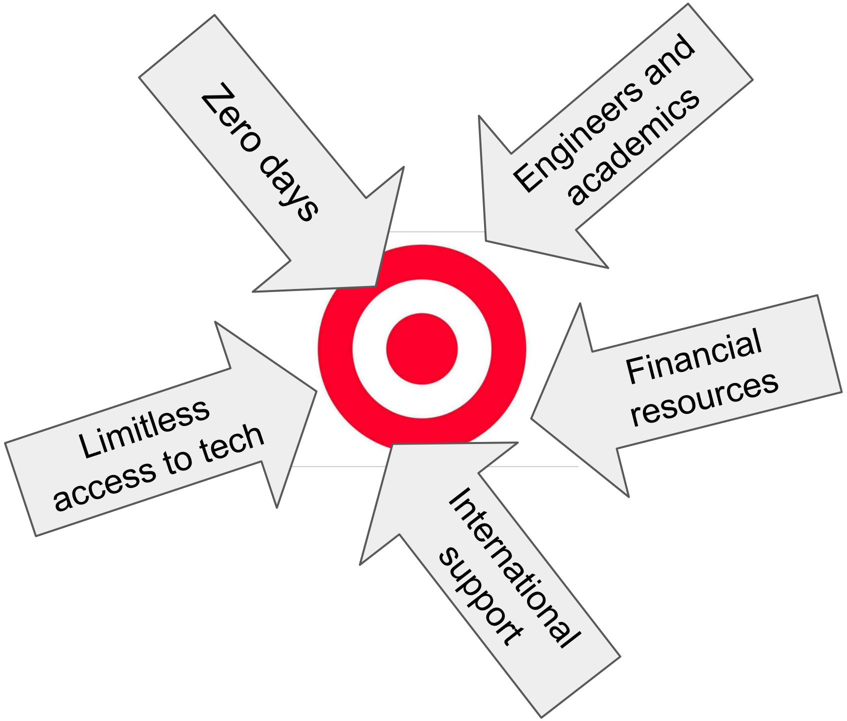
black/gray hat

People make mistakes

Known exploits

Generic and open source tools

Leaked tools



Zero days

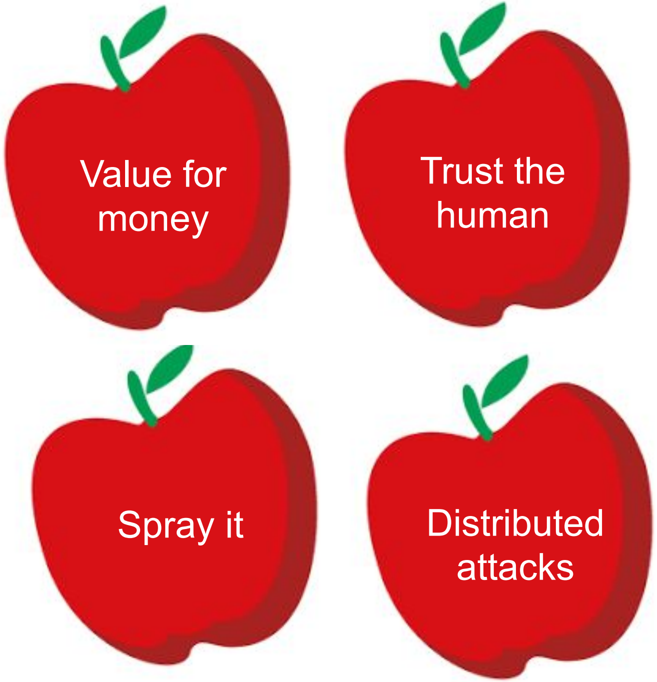
Engineers and academics

Limitless access to tech

Financial resources

International support

Methods

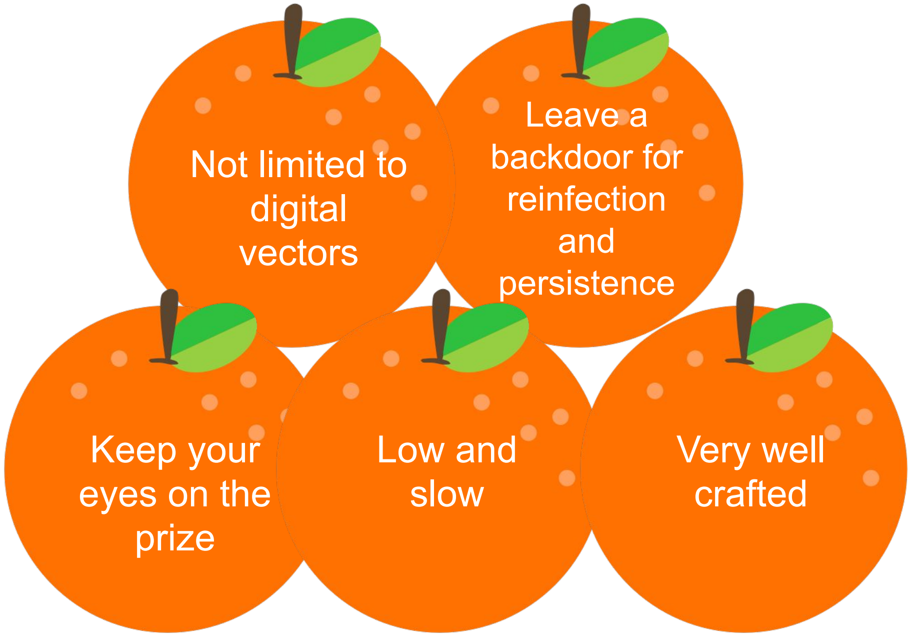


Value for money

Trust the human

Spray it

Distributed attacks



Not limited to digital vectors

Leave a backdoor for reinfection and persistence

Keep your eyes on the prize

Low and slow

Very well crafted

Main actors

North korea

Financial institutes, aerospace, chemicals, health, automotive, manufacturing

Iran

Financial institutes, government, energy, telecom, chemicals, aerospace

Russia

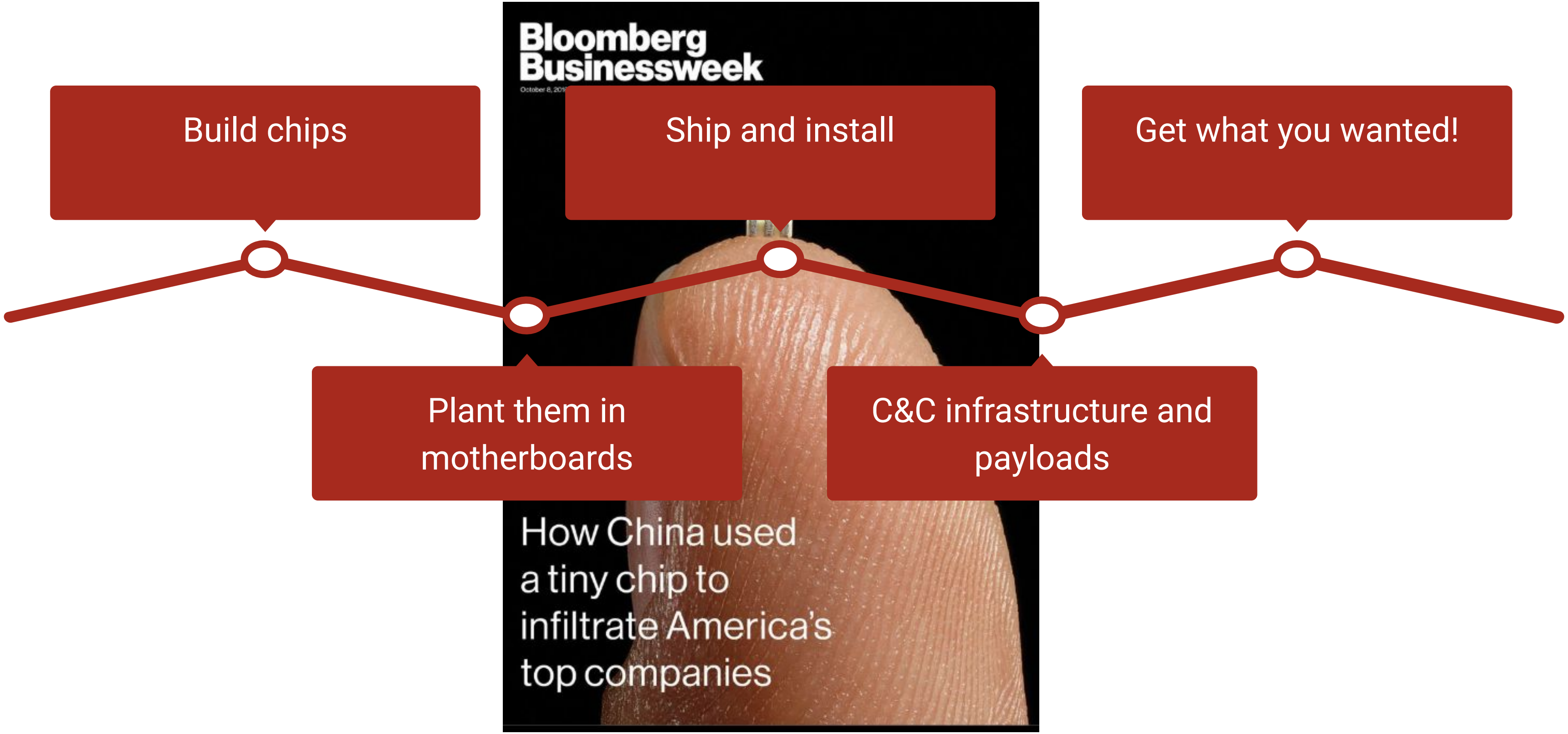
Governments, foreign policy orgs, military, NATO

China

Financial institutes, aerospace, engineering, military, tech, telcom, health, gov and legal, journalists

Images: FireEye

The best supply-chain attack ever! (that we know of)



Build chips

Plant them in motherboards

Ship and install

C&C infrastructure and payloads

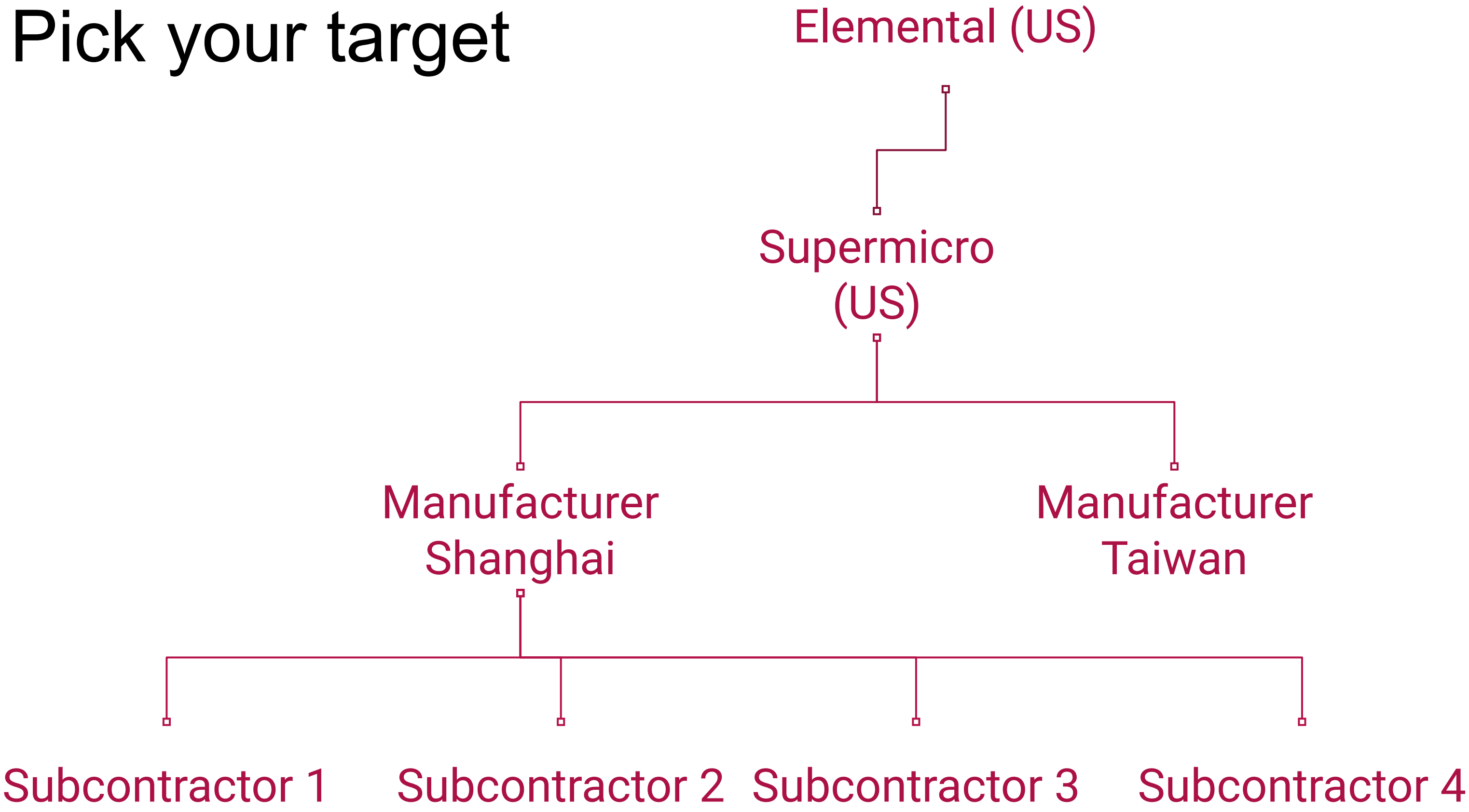
Get what you wanted!

Bloomberg Businessweek

October 8, 201

How China used a tiny chip to infiltrate America's top companies

Pick your target



Elemental (US)

Supermicro (US)

Manufacturer Shanghai

Manufacturer Taiwan

Subcontractor 1

Subcontractor 2

Subcontractor 3

Subcontractor 4

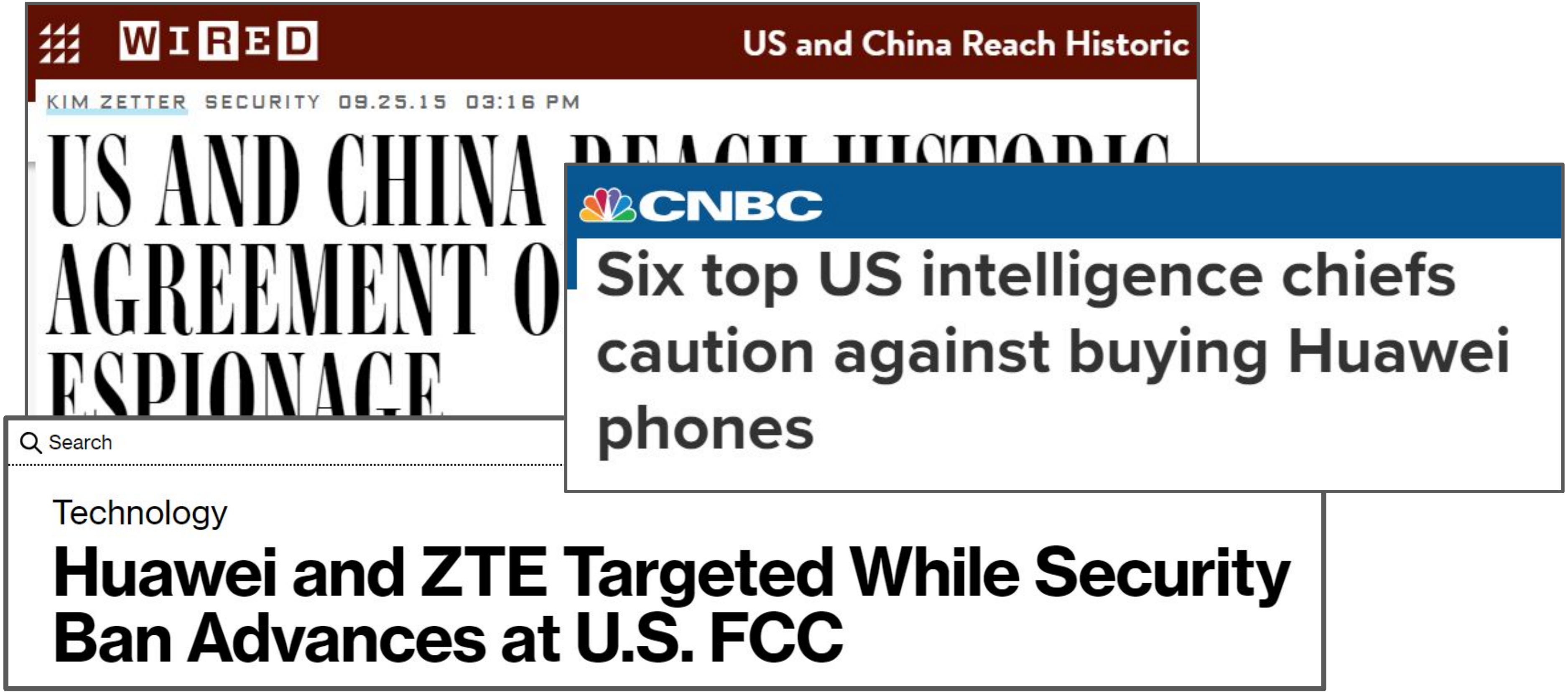
Kudos for this great operation!

Hardware is off the radar

(Almost) everyone manufacturers in China - great market analysis

Foot at the door everywhere, do anything you want - great technology

China - US relations



WIRED

US and China Reach Historic

KIM ZETTER SECURITY 09.25.15 03:16 PM

US AND CHINA REACH HISTORIC AGREEMENT O ESPIONAGE

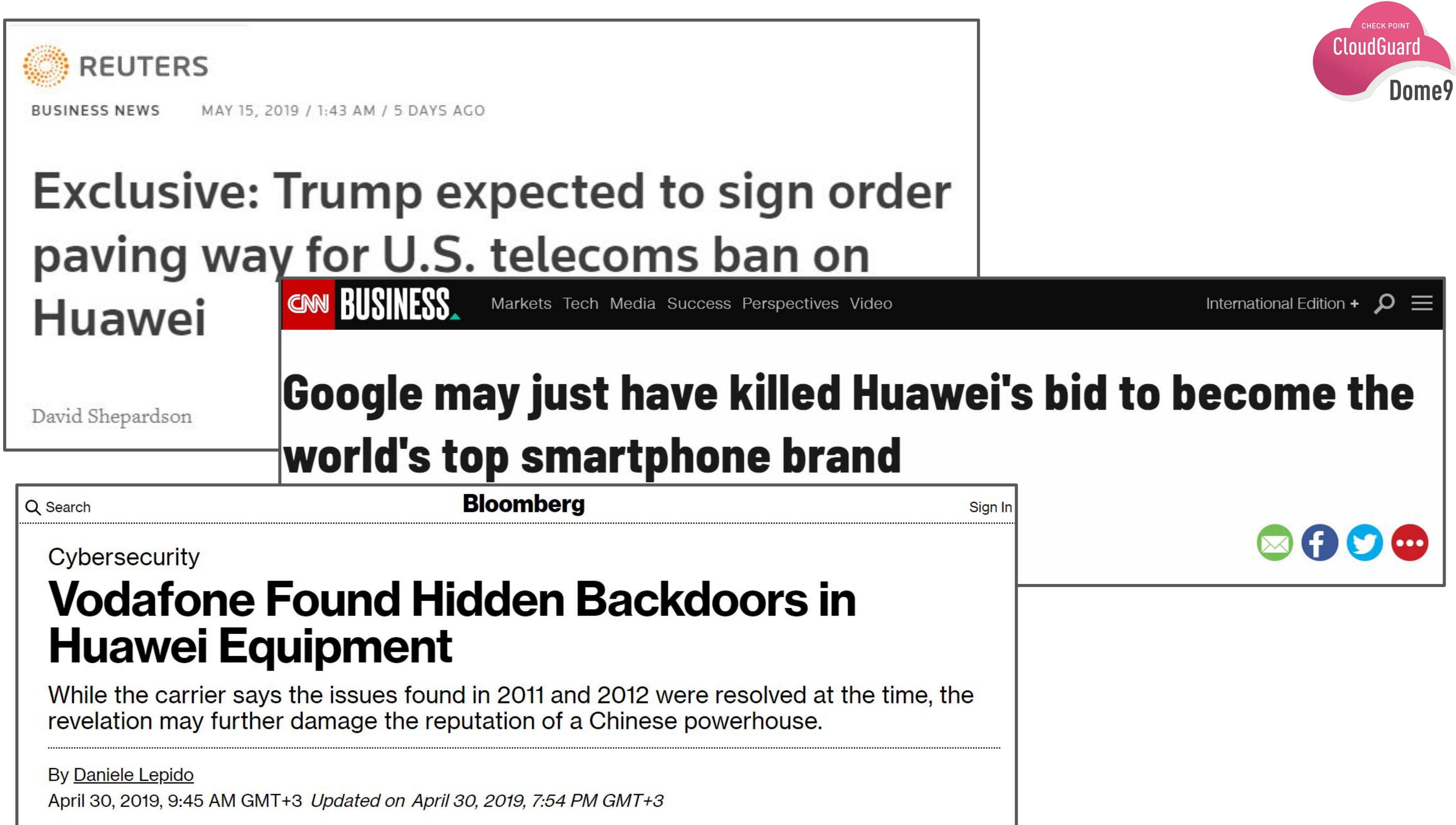
CNBC

Six top US intelligence chiefs caution against buying Huawei phones

Search

Technology

Huawei and ZTE Targeted While Security Ban Advances at U.S. FCC



REUTERS

BUSINESS NEWS MAY 15, 2019 / 1:43 AM / 5 DAYS AGO

Exclusive: Trump expected to sign order paving way for U.S. telecoms ban on Huawei

David Shepardson

Google may just have killed Huawei's bid to become the world's top smartphone brand

Cybersecurity

Vodafone Found Hidden Backdoors in Huawei Equipment

While the carrier says the issues found in 2011 and 2012 were resolved at the time, the revelation may further damage the reputation of a Chinese powerhouse.

By Daniele Lepido

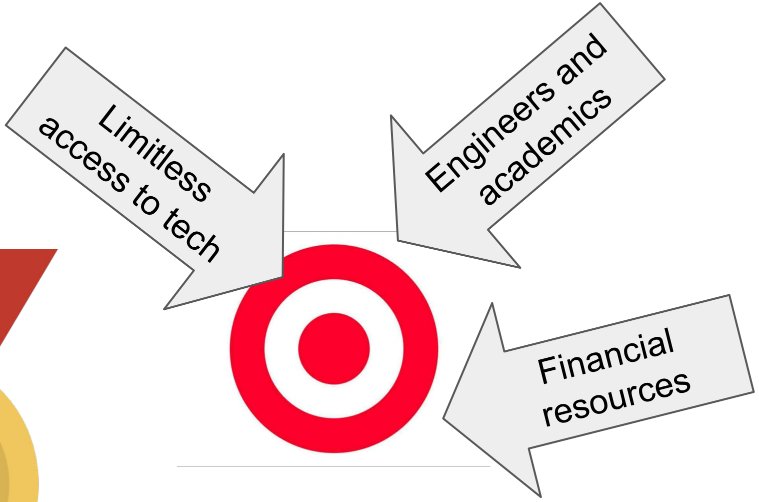
April 30, 2019, 9:45 AM GMT+3 *Updated on April 30, 2019, 7:54 PM GMT+3*

What did we see here?

Know all your secrets

Financial / trade advantage

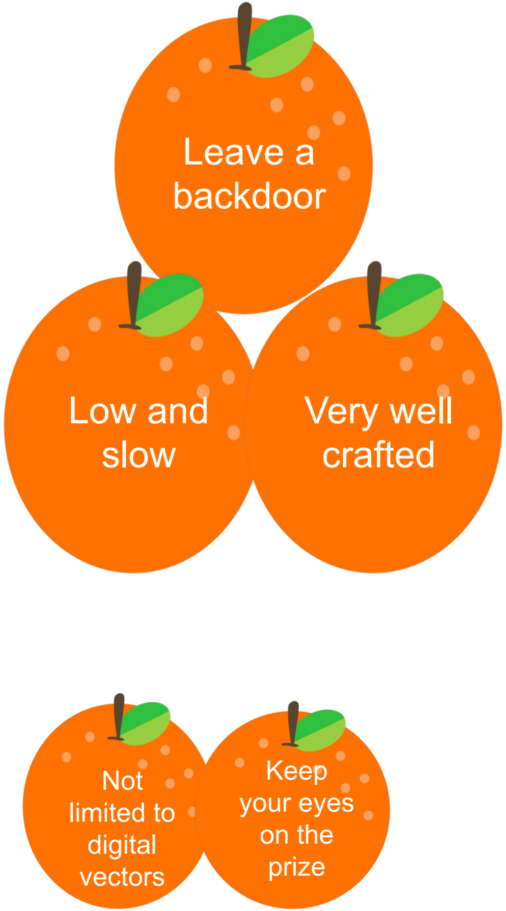
Easter egg



Limitless access to tech

Engineers and academics

Financial resources



Leave a backdoor

Low and slow

Very well crafted

Not limited to digital vectors

Keep your eyes on the prize

Where do you want to be

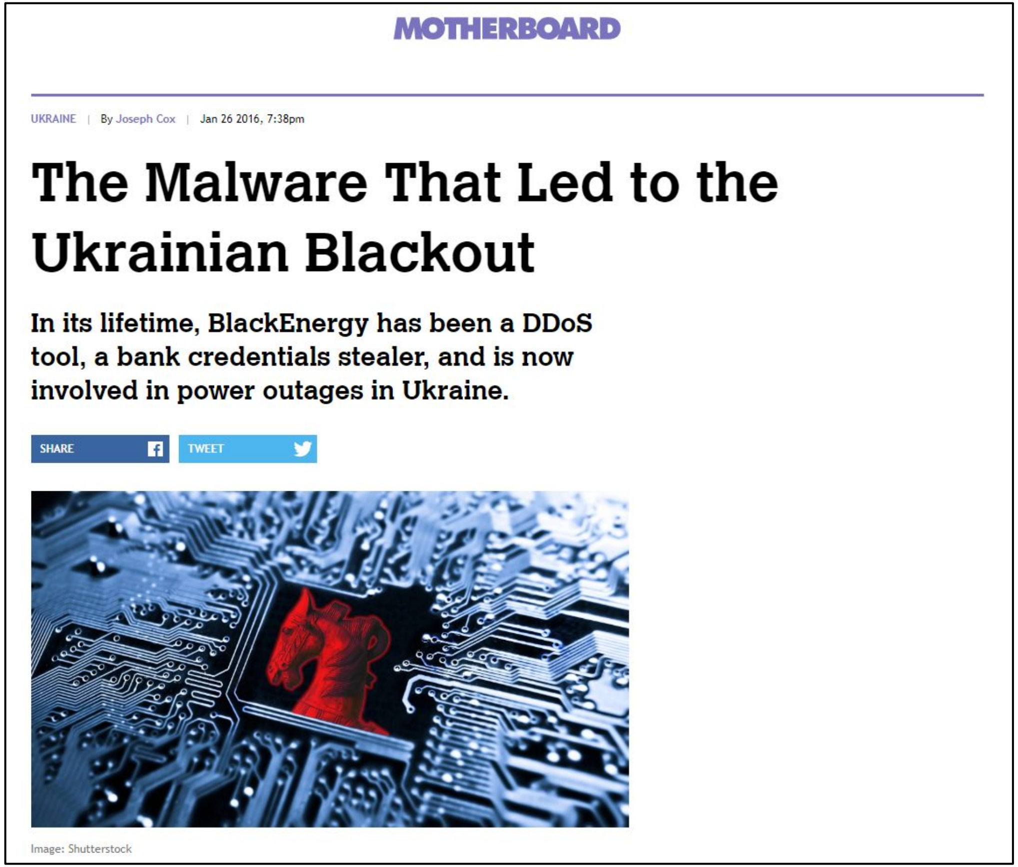
How to get there

What tools will get you there

Stay undetected

Take the time to plan

Who turned out the lights? (and why would they do that?)



MOTHERBOARD

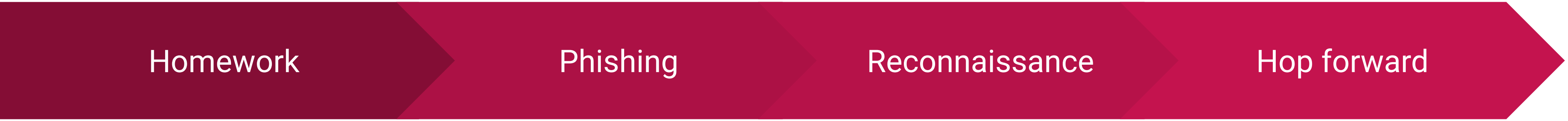
UKRAINE | By Joseph Cox | Jan 26 2016, 7:38pm

The Malware That Led to the Ukrainian Blackout

In its lifetime, BlackEnergy has been a DDoS tool, a bank credentials stealer, and is now involved in power outages in Ukraine.

Image: Shutterstock

To the target



Homework

- Who should you spearphish?
- What is going to make them open the email?

Phishing

- VERY well crafted emails
- Perhaps the sender wasn’t spoofed

Reconnaissance

- Lateral movement
- Credentials harvesting
- Privilege escalation
- Black Energy

Hop forward

- From management network to SCADA

At the target

Get the power down

Know the ICS
Take control

Get some damage done

Delete firmware
KillDisk

Bonus hack

DDoS to the phone operator

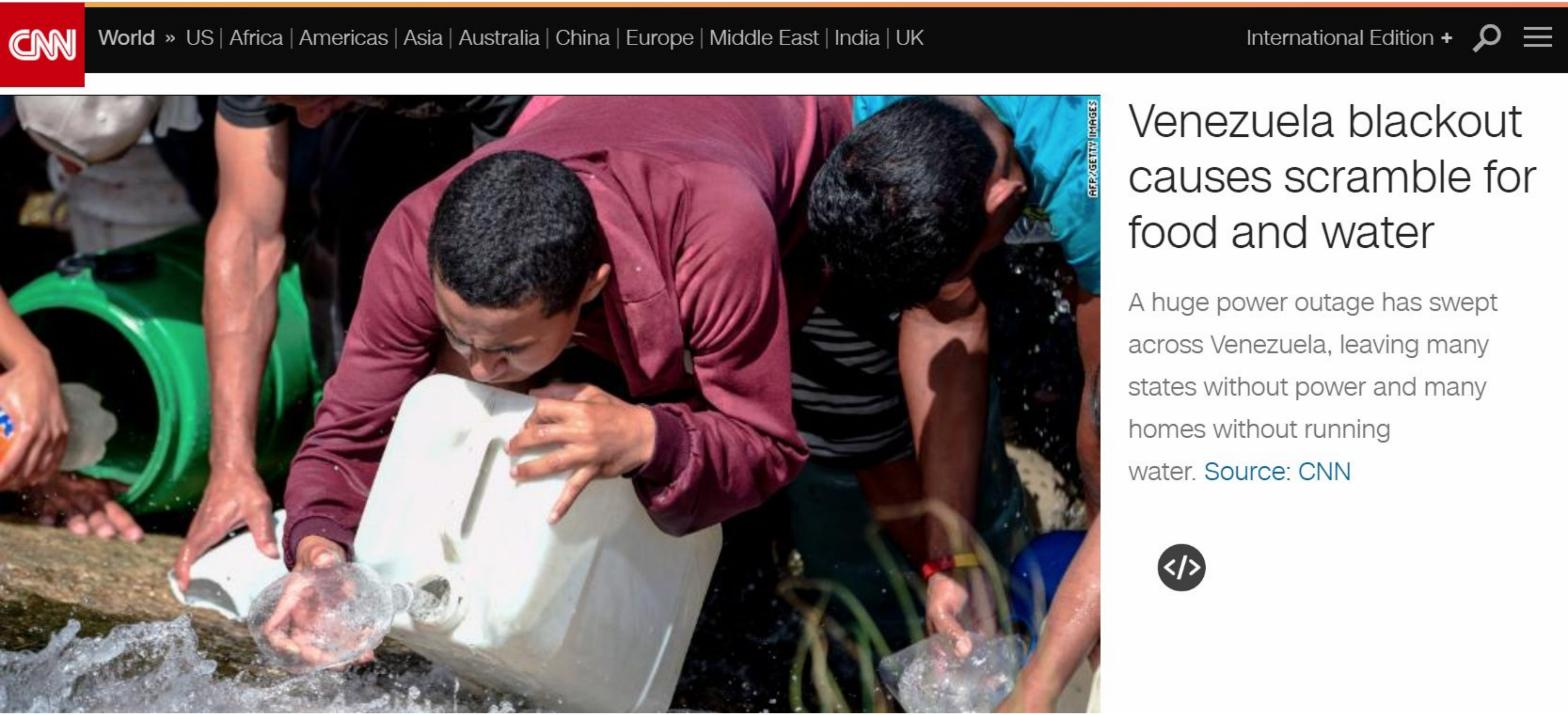
ПС Богородчани 110/35/10кВ
Well, what — he's [illegible] again,
with the 110 kW circuit

Another great operation!

Well synchronized

Understanding of the target

After effects

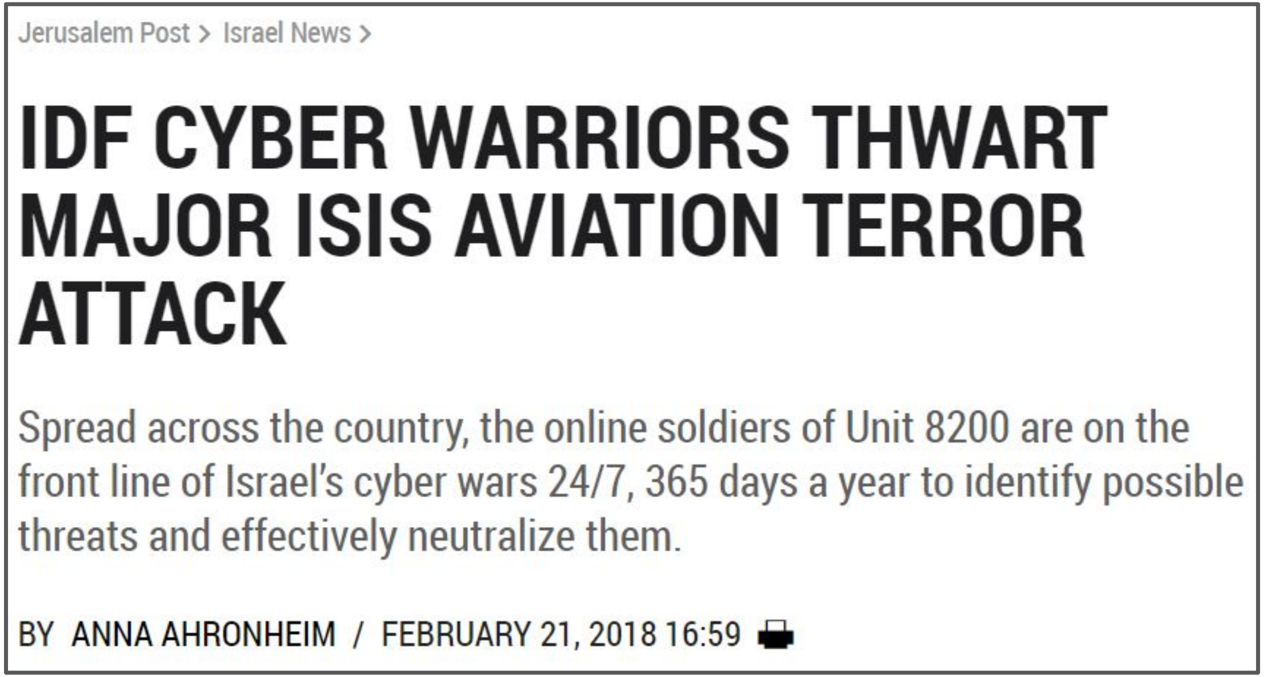

CNN
World » US | Africa | Americas | Asia | Australia | China | Europe | Middle East | India | UK
International Edition +
AFP/GETTY IMAGES

Venezuela blackout causes scramble for food and water

A huge power outage has swept across Venezuela, leaving many states without power and many homes without running water. Source: CNN

COUNTRIES OUT THERE THAT HAVE AN
INTEREST AND
GPS
FAREED ZAKARIA
IS RUSSIA MEDDLING IN UPCOMING UKRAINIAN ELECTIONS?
LIVE
CNN
7:42 AM PT
LIEVE WE HAVE THE SHOOTER IN CUSTODY FOR THIS INCIDENT, THE INVES
FAREED ZAKARIA GPS
VIZIO

Israel?

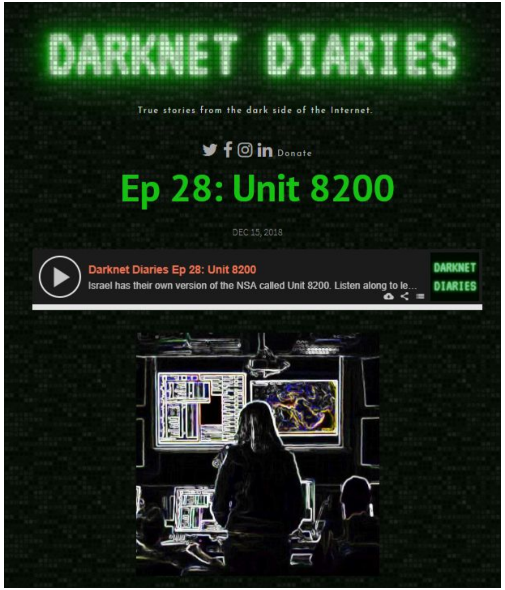


Jerusalem Post > Israel News >

IDF CYBER WARRIORS THWART MAJOR ISIS AVIATION TERROR ATTACK

Spread across the country, the online soldiers of Unit 8200 are on the front line of Israel's cyber wars 24/7, 365 days a year to identify possible threats and effectively neutralize them.

BY ANNA AHRONHEIM / FEBRUARY 21, 2018 16:59



DARKNET DIARIES

True stories from the dark side of the Internet.

Donate

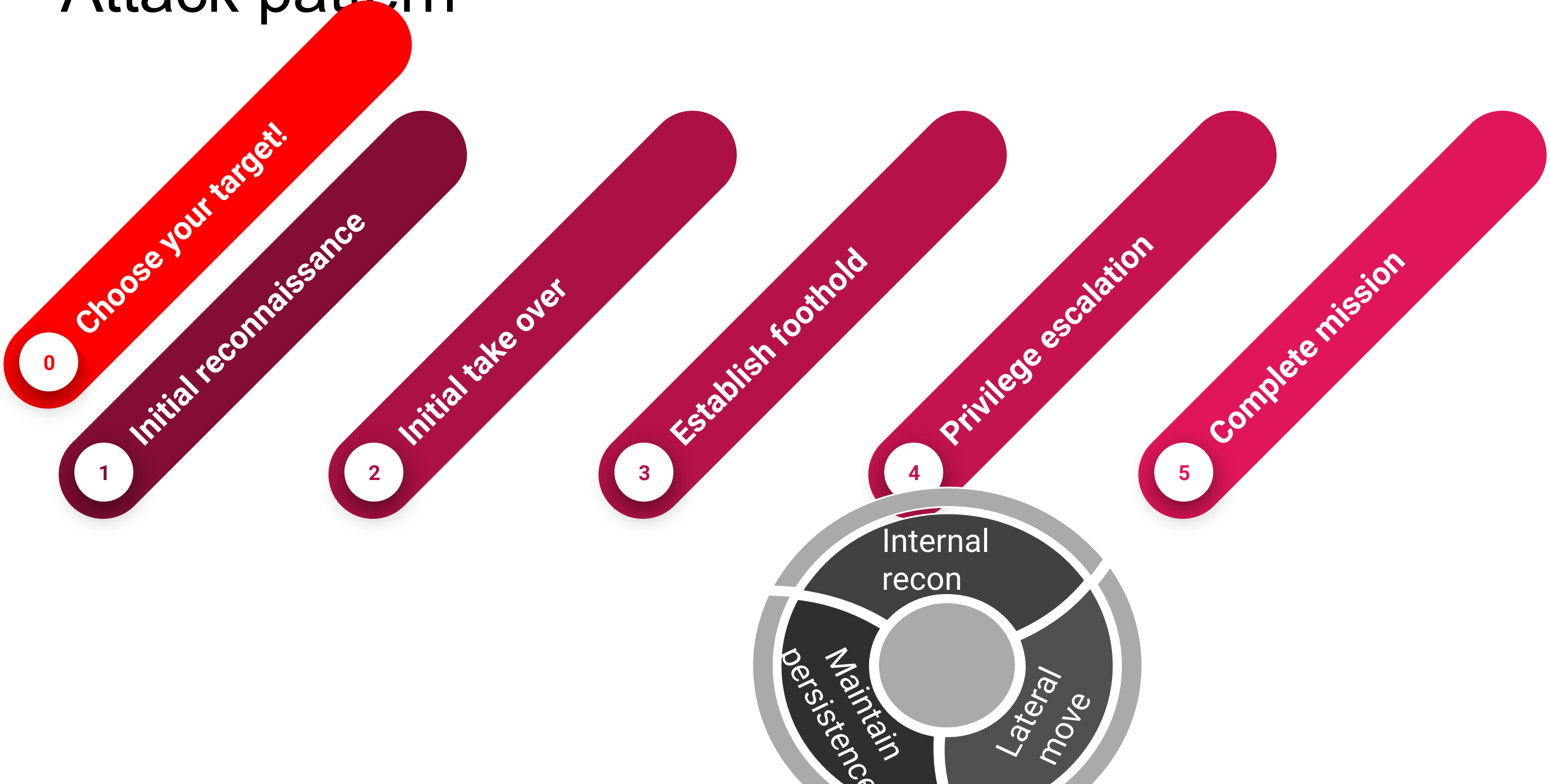
Ep 28: Unit 8200

DEC 15, 2018

Darknet Diaries Ep 28: Unit 8200

Israel has their own version of the NSA called Unit 8200. Listen along to le...

Attack pattern



0 Choose your target!

1 Initial reconnaissance

2 Initial take over

3 Establish foothold

4 Privilege escalation

5 Complete mission

Internal recon

Lateral move

Maintain persistence

Can we do anything about this?

More security?

Relate to this as an arm race?

Thank you!

Shira Shamban
@shambanIT