Vulnerabilities & Attacks

Paolo PRINETTO
Director
CINI Cybersecurity National Laboratory
Paolo.Prinetto@polito.it
Mob. +39 335 227529

cini
Cybersecurity
National Lab

www.consorzio-cini.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Acknowledgments

Thanks

- The presentation includes material from several contributors, whose valuable help is here acknowledged and highly appreciated.

Contributors

- CyberChallenge.IT
- Giuseppe AIRO' FARULLA
- Alessandro ARMANDO
- Roberto BALDONI
- Rocco DE NICOLA
- Arturo DI CORINTO
- Giorgio DI NATALE
- Eugene KASPERSKY
- Rosario PUGLIESE
- Francesco VESTITO
- Stefano ZANERO

Outline

- Vulnerabilità
- Attacchi
- Classi di attacco
- Superfici di attacco
- Tipi di minaccia

Outline

- Vulnerabilità
- Attacchi
- Classi di attacco
- Superfici di attacco
- Tipi di minaccia

Vulnerabilità

- La complessità genera *vulnerabilità*

Vulnerabilità

- *Debolezza* presente in una delle componenti di un sistema che può essere sfruttata da un attaccante per condurre un *attacco* contro il sistema stesso

Componenti di un sistema

- Aspetti organizzativi
- Aspetti tecnologici (Hardware/Software)
- Fattore umano

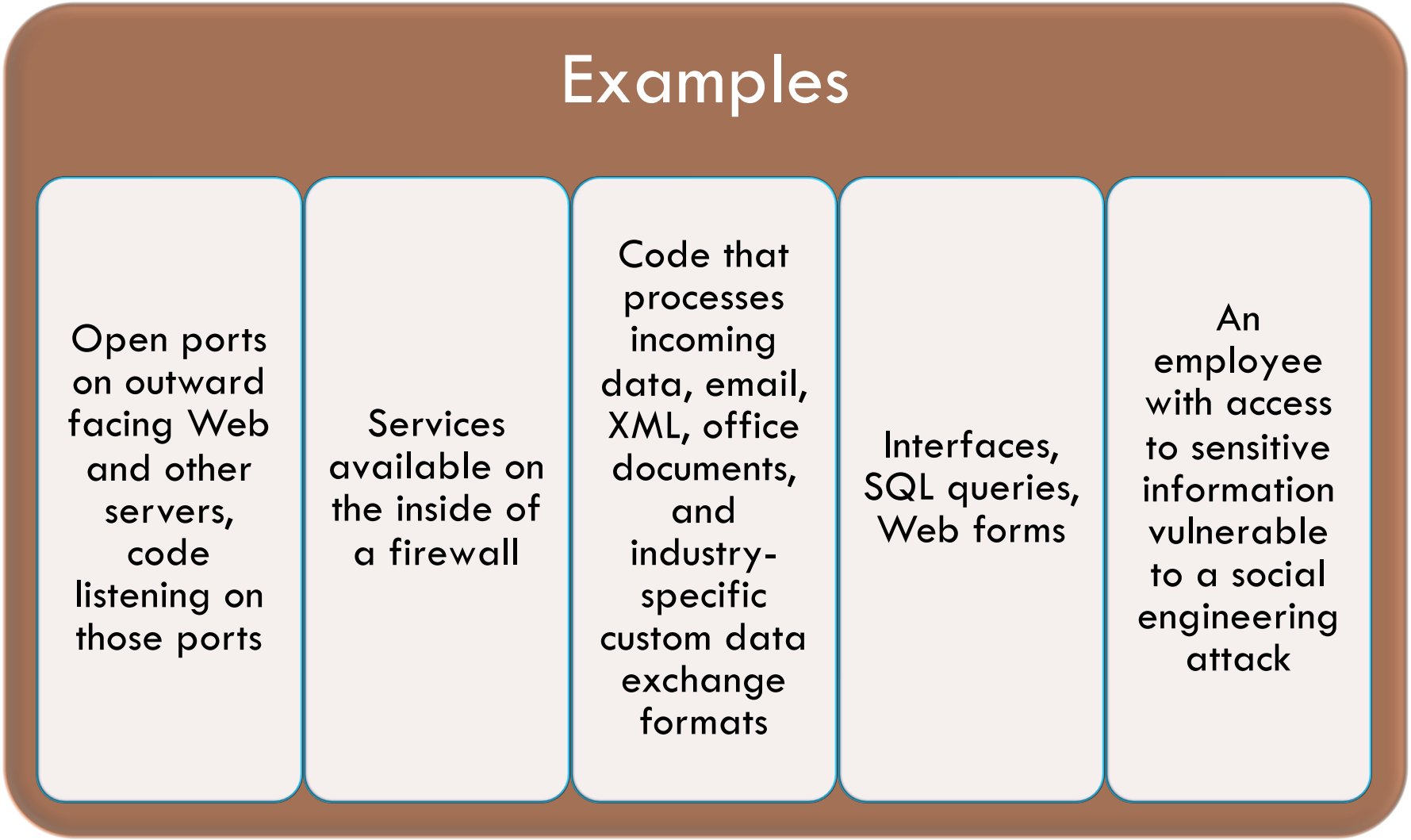
Ranking

Ranking

Vulnerabilità derivanti dagli aspetti tecnologici - Cause

- Bachi nei programmi
- Errori di progettazione dell'hardware
- *Leggerezze* in fase di progettazione
- Errate configurazioni
- Debolezze nei protocolli
- …

Some reachable and exploitable vulnerabilities in a system



Outline

- Vulnerabilità
- Attacchi
- Classi di attacco
- Superfici di attacco
- Tipi di minaccia

Attacchi

- Le *vulnerabilità* e il *fattore umano* sono sfruttati dai cyber-criminali per sferrare *attacchi*

Finalità degli Attacchi

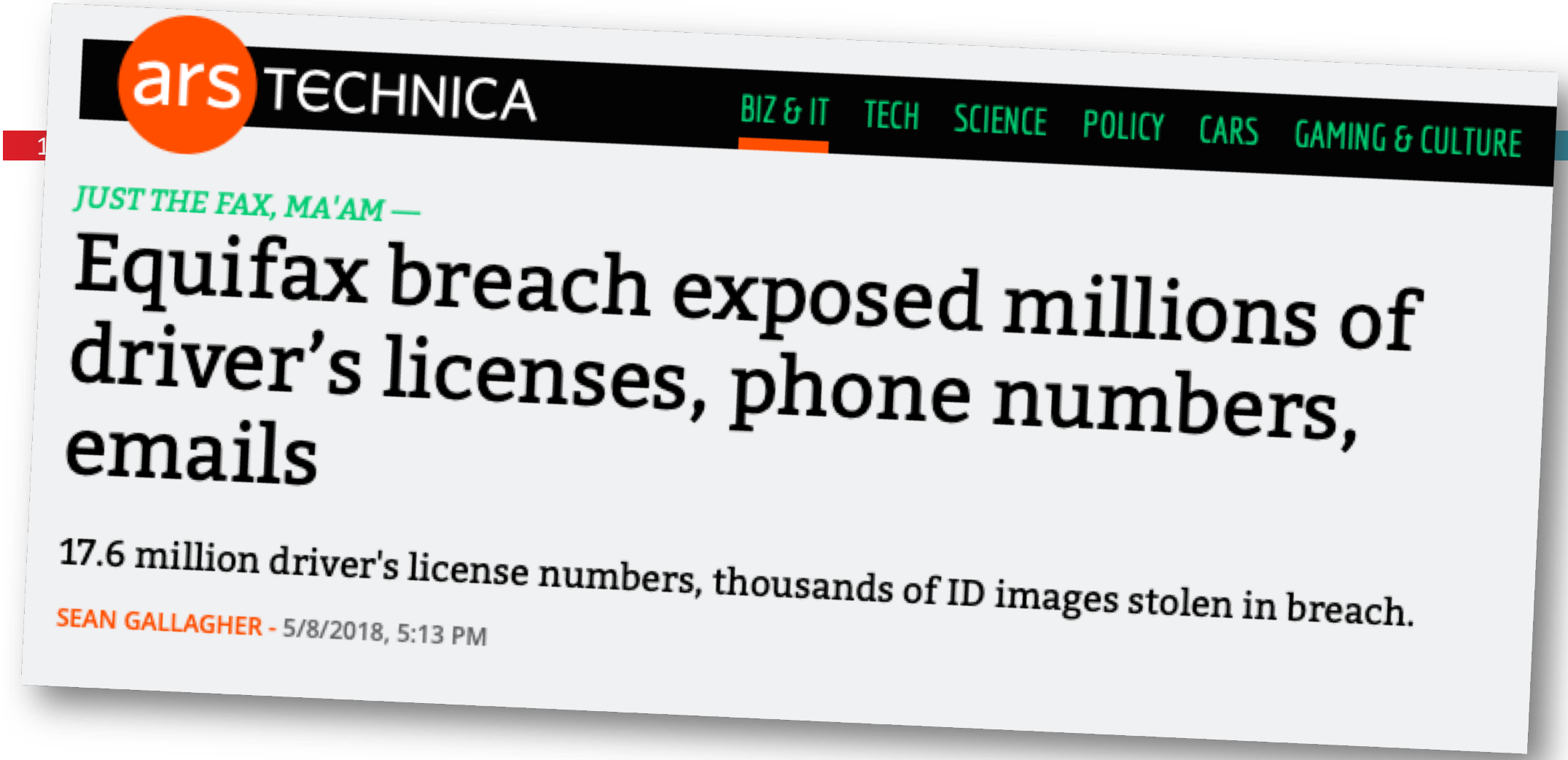
- Gli *attacchi* mirano a:

Finalità degli Attacchi

- Gli *attacchi* mirano a:
  - esfiltrare dati
  - rubare soldi/oggetti
  - arrecare danni
  - controllare in modo surrettizio strutture, servizi e intere nazioni
  - …

Finalità degli Attacchi

- Gli *attacchi* mirano a:
  - esfiltrare dati
  - rubare soldi/oggetti
  - arrecare danni
  - controllare in modo surrettizio strutture, servizi e intere nazioni
  - …



ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

JUST THE FAX, MA'AM —

Equifax breach exposed millions of driver's licenses, phone numbers, emails

17.6 million driver's license numbers, thousands of ID images stolen in breach.

SEAN GALLAGHER - 5/8/2018, 5:13 PM

Home | Politica | Economia | Sport | Spettacoli | Tecnologia | Motori | Tutte le sezioni | D | Rep tv

Hackerata la catena di hotel Marriott: a rischio i dati di 500 milioni di clienti

(reuters)

La compagnia ha annunciato di aver subito un attacco informatico ai suoi database. Potenzialmente coinvolti mezzo miliardo di utenti che hanno soggiornato negli albertghi del gruppo dal 2014 a oggi


CloudPets
THE INTERNET OF HACKABLE THINGS
Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings
LORENZO FRANCESCHI-BICCHIERAI
Feb 27 2017, 10:00pm
A company that sells "smart" teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.
UPDATE, Feb. 28, 12:25 p.m. ET: After this story was published, a security researcher revealed that the stuffed animals themselves could easily be hacked


ASHLEY MADISON®
Life is short. Have an affair.®
See Your Matches »
READ MORE
Ashley Madison hack reveals its 37 million users sexual fantasies

Rubate le mail a 1,4 milioni di utenti Libero e Virgilio

Il cybercriminale, uno studente di 24anni, si è intrufolato nella rete Wi-Fi del gestore (Italiaonline) operando da un bar vicino alla sede dell'azienda (Assago, Milano). I carabinieri l'hanno fermato dopo che aveva già spedito il pacchetto di credenziali mail al committente

Finalità degli Attacchi

- Gli *attacchi* mirano a:
  - esfiltrare dati
  - rubare soldi/oggetti
  - arrecare danni
  - controllare in modo surrettizio strutture, servizi e intere nazioni
  - …

SICUREZZA INFORMATICA

Hacker rubano 36 milioni di euro sui conti di 30 banche europee via sms

Colpiti anche clienti italiani. L'attacco attraverso un trojan dormiente sui Pc che si è trasferito sugli smartphone

(Foto web)

Oltre 36 milioni di euro, sui conti di 30 banche europee. Una cifra da capogiro. Rubata da un gruppo di hacker anche di clienti italiani. A darne notizia è stato il Financial Times nell'edizione online, rilevando che si tratterebbe del primo caso di furto che ha preso specificatamente di mira le procedure di sicurezza sui servizi

NOTIZIE CORRELATE

- L'attacco di Apple: «Android è a rischio» (22/01/2014)

cini Cybersecurity National Lab

R.it | Cronaca

Home | Politica | Economia | Sport | Spettacoli | Tecnologia | Motori

Mr. Confindustria a Bruxelles truffato da un hacker: persi 500mila euro. Licenziato

"Sposta subito mezzo milione su questo conto estero". Ma la mail era di un hacker. E i soldi sono spariti. Il finto ordine a firma della direttrice Panucci: "Esegui e non mi chiamare che sto fuori col presidente"

di ROBERTO MANIA

Lo leggo dopo | 30 settembre 2017

Gianfranco Dell'Alba

ROMA - Ci sono circa cinquecentomila euro che da un conto della Confindustria sono finiti in un conto estero di cui ancora non si conosce l'intestatario. Soldi evaporati, per ora. C'è una mail falsa da cui è cominciato tutto. C'è un dirigente dell'associazione degli industriali licenziato in tronco per un bonifico che non avrebbe dovuto fare. È successo in Confindustria ma sono centinaia le aziende colpite ogni giorno da frodi finanziarie e milioni le mail contraffatte (mail spoofing, le chiamano gli esperti del settore) da cui partono ordini per spostare denaro in ogni parte del mondo.

Hacker truffa con una mail falsa un dirigente di Confindustria: spariti 500mila euro

"Sposta subito mezzo milione su questo conto estero". Il finto ordine a firma della direttrice Marcella Panucci, ad eseguire il bonifico il dirigente livornese Gianfranco Dell'Alba

TRUFFE | CONFINDUSTRIA | HACKER

30 settembre 2017

ADVANCED CROSS-BORDER FINANCIAL CYBERCRIME

CARBANAK — THE $1 BILLION BANK HEIST

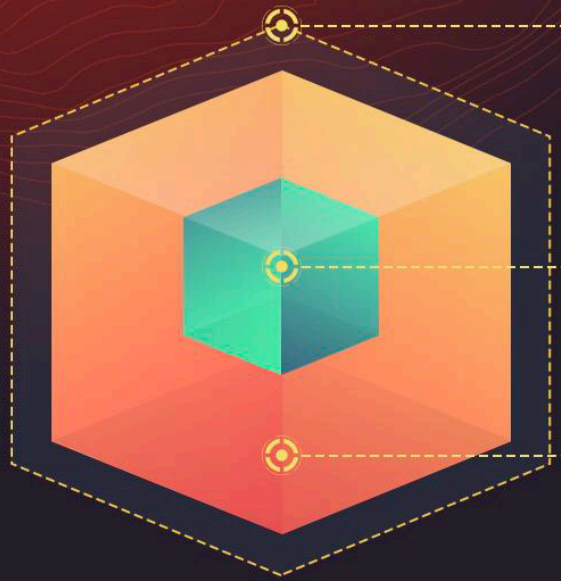
Infecting bank clerks' computers

Harvesting intelligence

Controlling admin computers

Stealing money

BANGLADESH CENTRAL BANK HEIST



35 transfer orders to the New York Federal Reserve

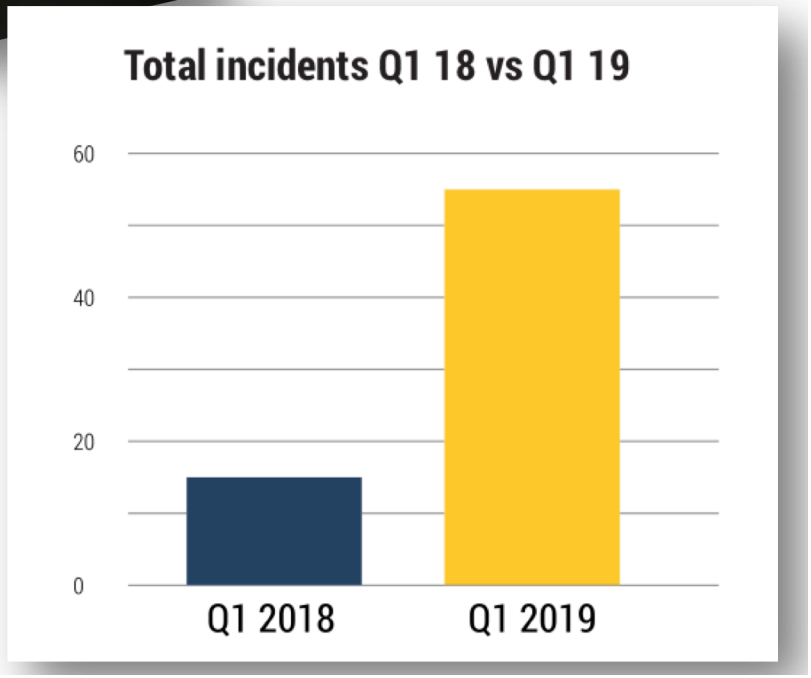
Four orders, $81M
Stolen, still missing

31 orders, $870M
Blocked because of word 'Fandation'

[E. Kaspersky, 2018]

Upstream

Q1 2019 SEES RAPID GROWTH OF AUTOMOTIVE CYBER INCIDENTS

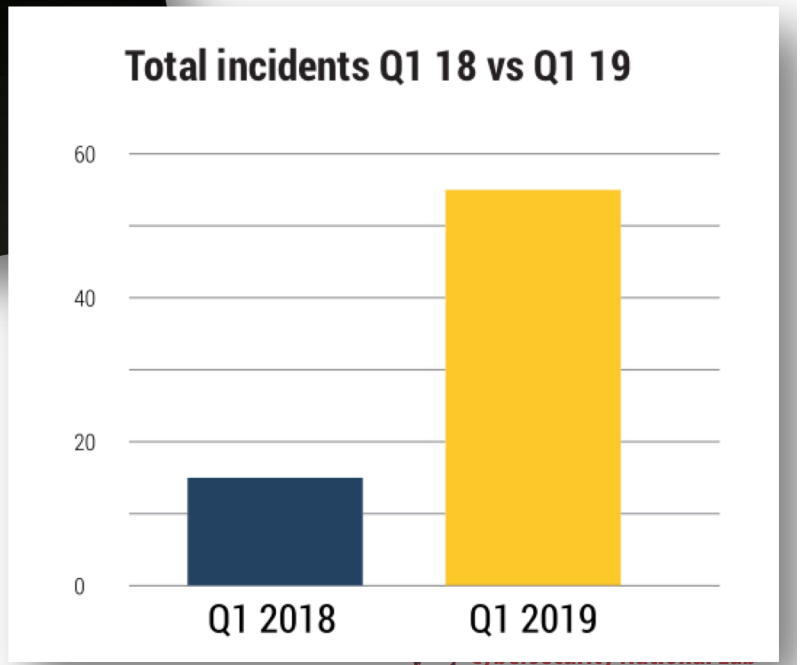


Automotive attacks

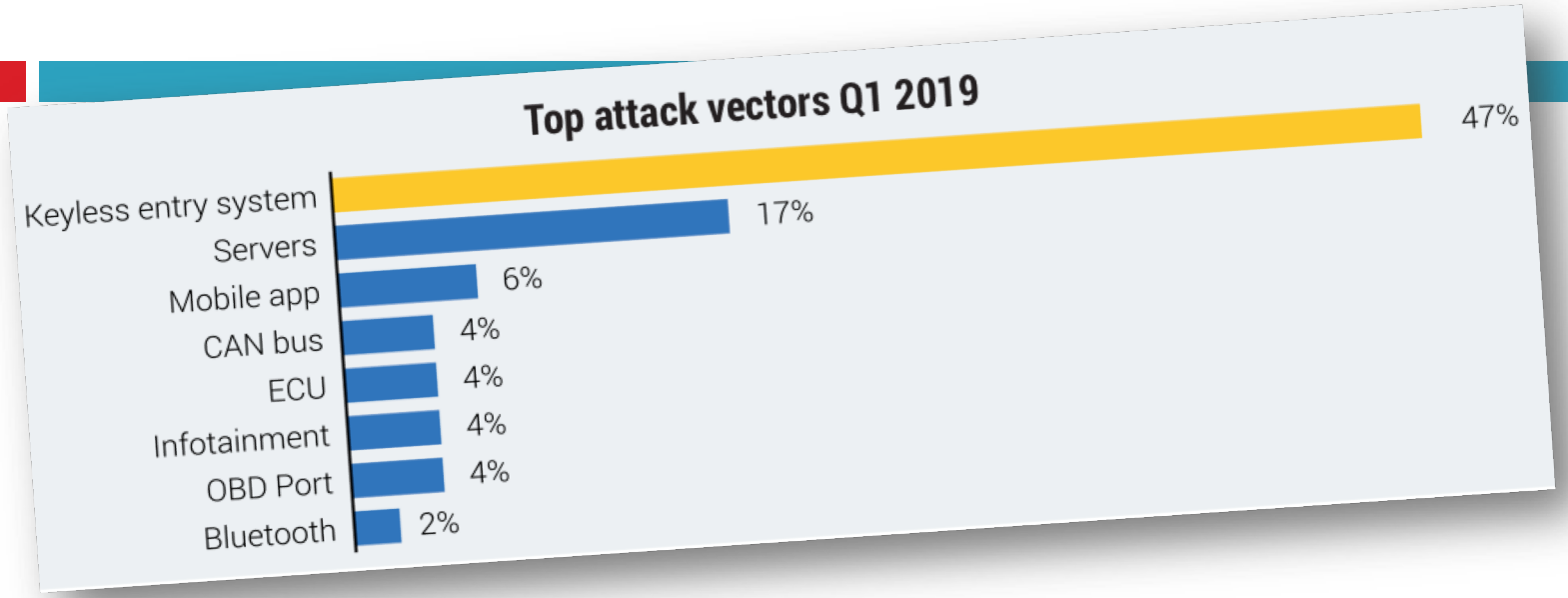
Automotive attacks

Upstream

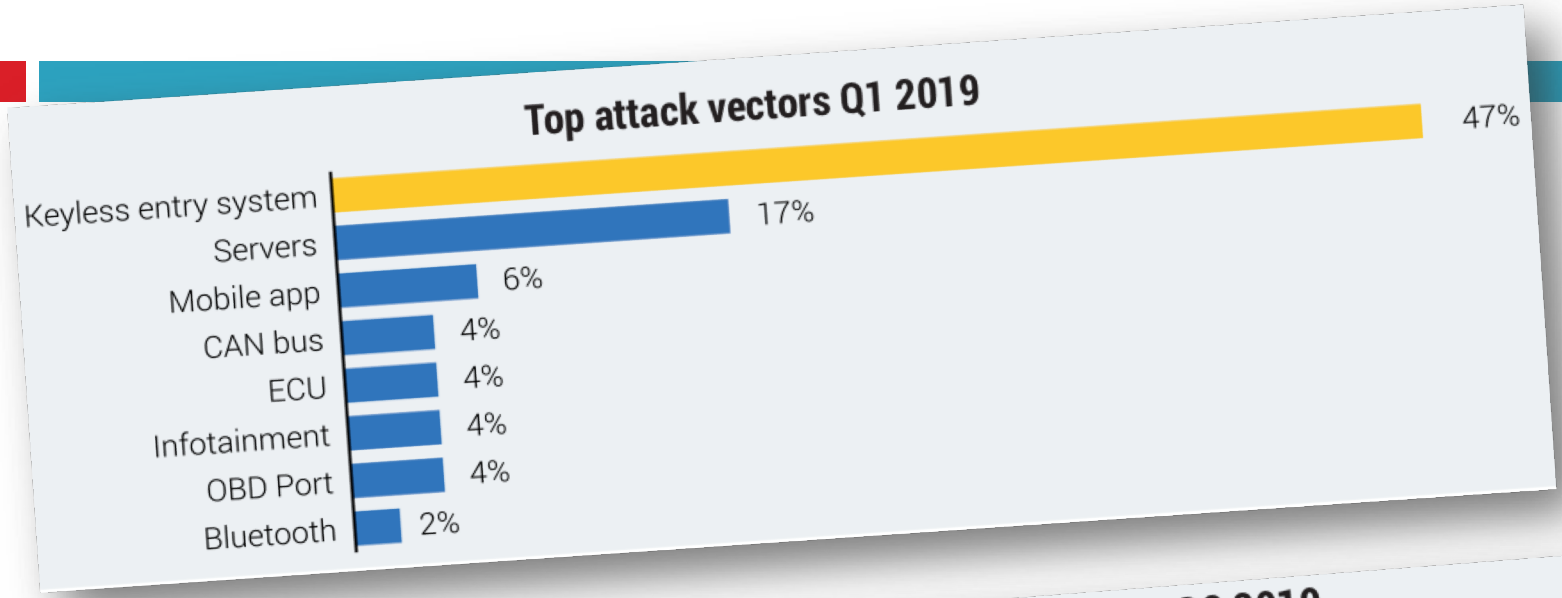
Q1 2019 SEES RAPID GROWTH OF AUTOMOTIVE CYBER INCIDENTS

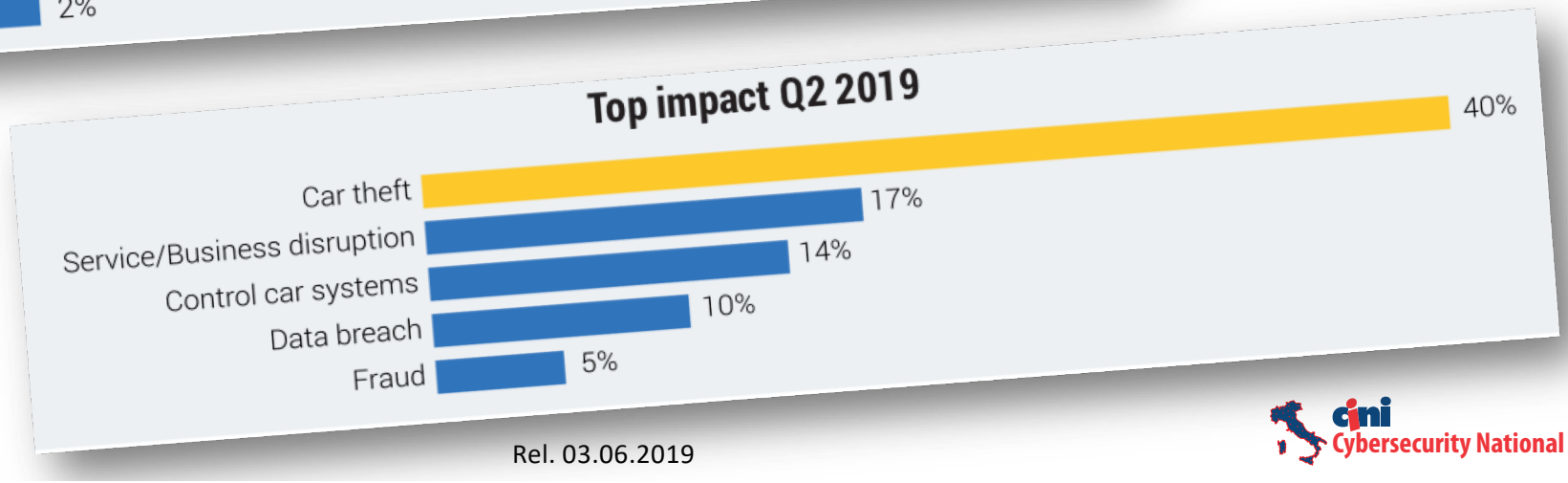


Automotive attacks



Automotive attacks





Finalità degli Attacchi

- Gli *attacchi* mirano a:
  - esfiltrare dati
  - rubare soldi/oggetti
  - arrecare danni
  - controllare in modo surrettizio strutture, servizi e intere nazioni
  - …

Attacco DDoS Contro Dyn DNS, giù twitter, spotify, github, heroku e altri.

I Cyber attacchi si fanno sempre più frequenti e rappresentano giorno per giorno una grave minaccia per le compagnie IT.

Surveillance Camera Attack

- A massive Distributed Denial of Service (DDoS) attack slowed down major websites
  - Twitter, Spotify, Amazon, Reddit, Yelp, Netflix, and The New York Times
- Target: Dyn (a major DNS host)
- Attack: a weakness in surveillance cameras, that allowed installing malicious software in more than 25,000 cameras!

PRIVACY AND SECURITY FANATIC

By Ms. Smith, Network World | FEB 12, 2017 8:15 AM PT

University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices

A university, attacked by its own malware-laced soda machines and other botnet-controlled IoT devices, was locked out of 5,000 systems.

About

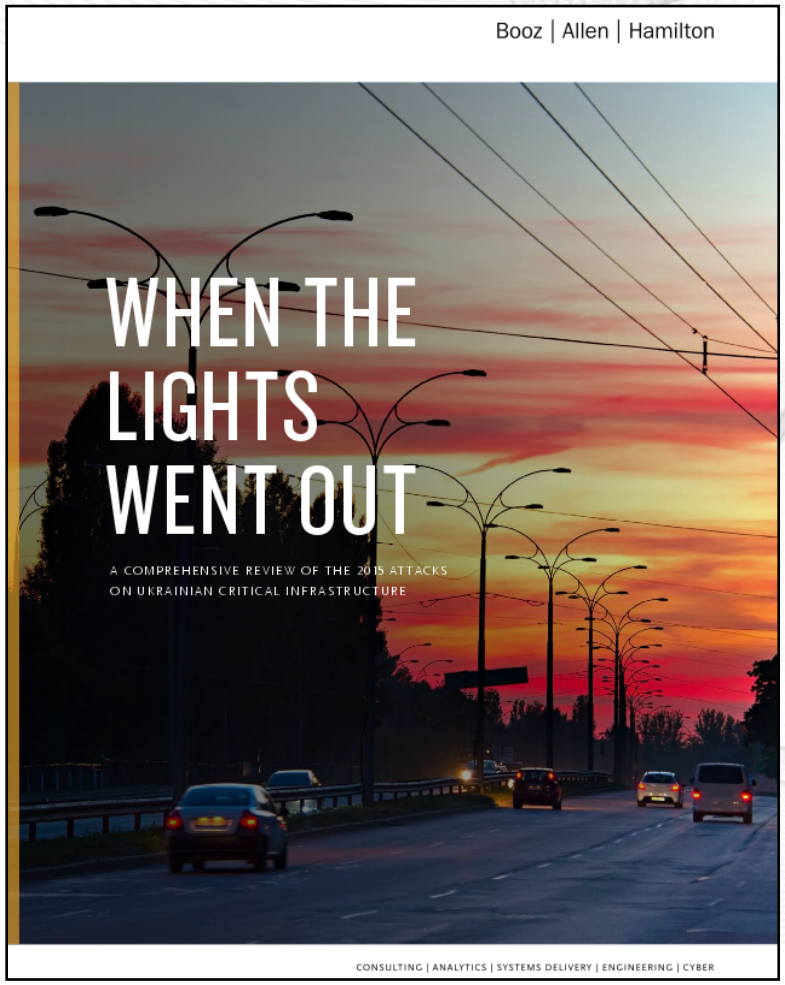
Ms. Smith (not her real name) is a freelance wr
programmer with a special and somewhat per
interest in IT privacy and security issues.

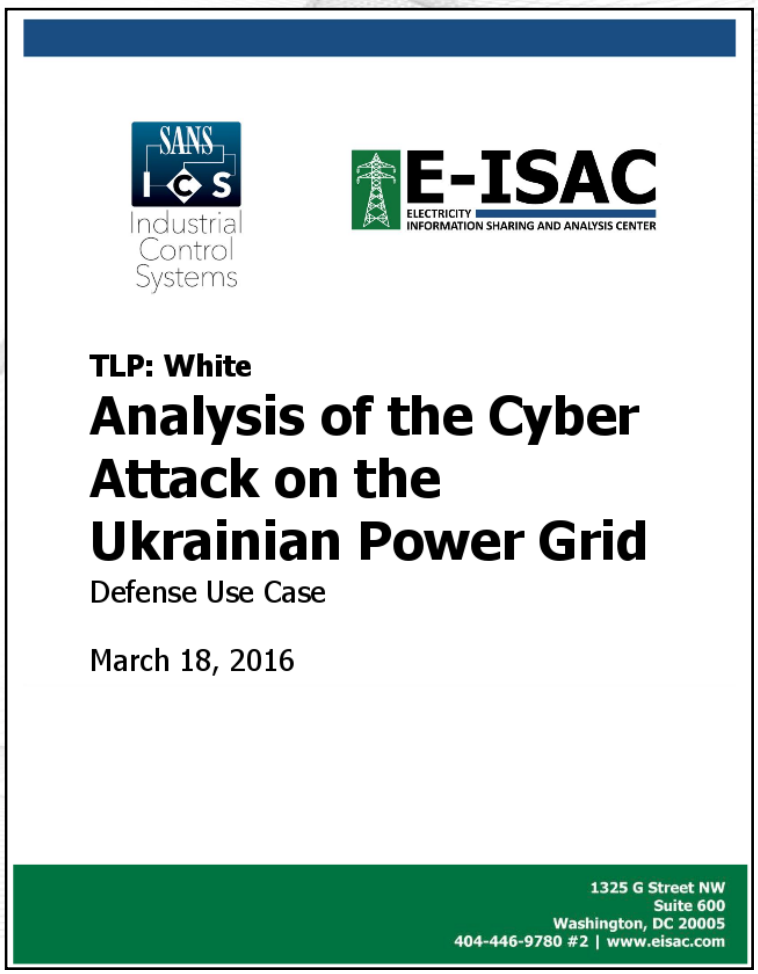
HACKING | Di Joseph Cox | gen 12 2016, 10:18am

La rete elettrica in Ucraina è stata attaccata da degli hacker

Gli hacker hanno attaccato anche i centri telefonici cercando di impedire ai clienti di notificare alle compagnie le interruzioni di corrente.

ANALISI DELLA MINACCIA





e-gazette.it

Notiziario ambiente energia on-line dal 1999

CYBERATTACCO, UN VIRUS INFORMATICO PROVOCA BLACKOUT IN UCRAINA

KIEV (UCRAINA) LUN, 11/01/2016

1

Grazie a un documento Excel infetto, il 23 dicembre scorso 700mila persone sono rimaste al buio per diverse ore

Il tanto temuto blackout provocato da attacco informatico alle centrali elettriche è arrivato. Il primo vero salto di qualità nelle minacce hacker ad impianti elettrici è avvenuto il 23 dicembre scorso, ai danni della rete elettrica ucraina nel Nord-Ovest del Paese: lo ha reso noto l'azienda di sicurezza informatica Eset, sottolineando come si tratti del primo caso del genere al mondo. Secondo Eset, il virus responsabile dell'attacco è stato infiltrato nel sistema grazie a un documento Excel infetto: si tratta di un programma denominato "BlackEnergy", contenente a sua volta un eseguibile, "KillDisk", in grado di sabotare le funzionalità dei sistemi industriali, spesso assai vulnerabili.

Nel capoluogo della regione Ivano/Frankivsk sono rimasti senza luce circa 700mila persone. L'interruzione della corrente - leggiamo su International Business Time - è durata circa sei ore. "Se questo è veramente il primo attacco riuscito contro impianti elettrici, credo che un sacco di persone lo interpreteranno come il passaggio del Rubicone" ha detto Jason Healy, esperto di conflitti informatici e ricercatore senior presso la Columbia University's School of International and Public Affairs di New York. "Non c'è dubbio che il rischio aumenta ogni anno e che tali attacchi saranno sempre più comuni."

I funzionari ucraini hanno aperto un'inchiesta su quell'evento ed alcuni studi recenti sottolineano che l'attacco avrebbe colpito almeno altre due utility in Ucraina occidentale. Secondo le spiegazioni fornite dai tecnici, BlackEnergy esiste da circa un decennio e in passato è stato utilizzato per attacchi hacker da parte del gruppo Sandworm, con sede a Mosca e vicino al governo russo.

Nonostante l'esistenza di responsabilità provate e circostanziate c'è una certa titubanza nell'attribuire la colpa a un partito politico. Un istruttore certificato di sicurezza informatica sostiene che occorrono più analisi per poter giungere ad una conclusione, soprattutto perché si tratta di infrastrutture civili fuori dalle zone del conflitto. Tuttavia, come alcuni stati utilizzano l'informatica per spiarsi l'un l'altro, gli stessi potrebbero arrivare a trovarsi in posizioni scomode nell'ammettere le azioni di spionaggio.

LA COMUNICAZIONE

Ascolta

IoT security, 350 mila pacemaker a rischio attacchi informatici negli USA

Intervento della Food and drug administration: batterie scarse e bassi livelli di cybersecurity. Solo l'anno passato sono state individuate oltre 8.000 vulnerabilità su sette diversi apparecchi.

di **Flavio Fabbri** | @FabbriFlav2 | 8 maggio 2018, ore 12:21

ANALISI DELLA MINACCIA

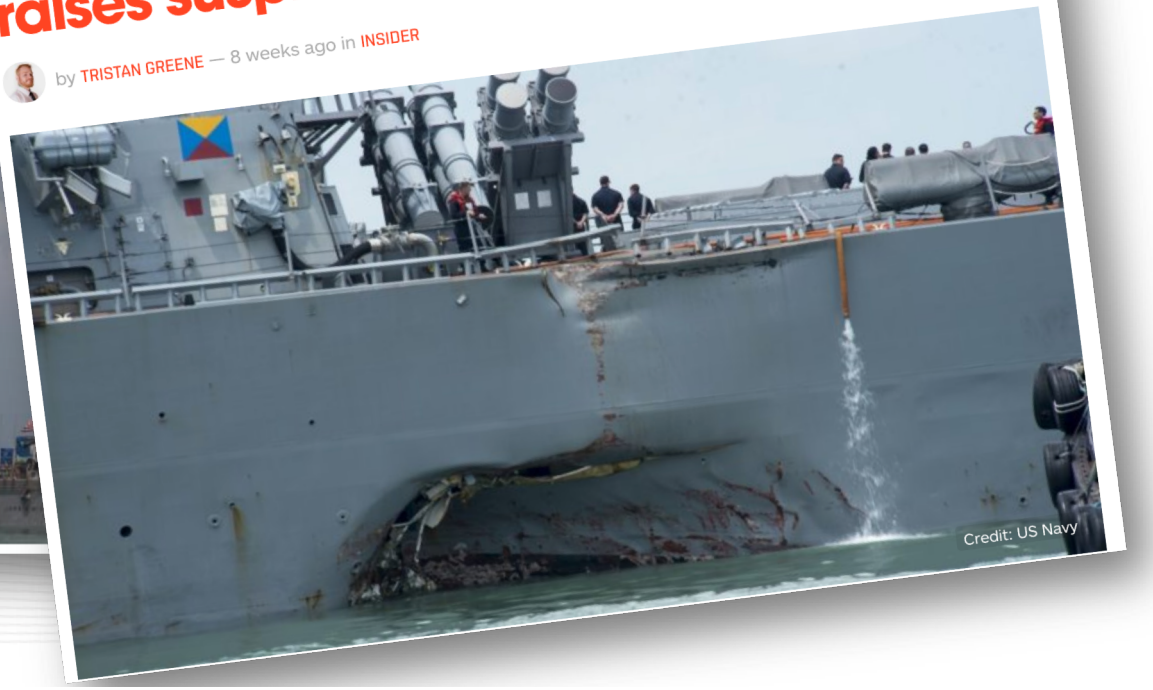
Hacking link to USS McCain warship collision? Expert says 'I don't believe in coincidence'

THE collision of a second US warship this year that has left 10 sailors missing points to the possibility of cyber-
an expert has warned.

Charis Chang @CharisChang2

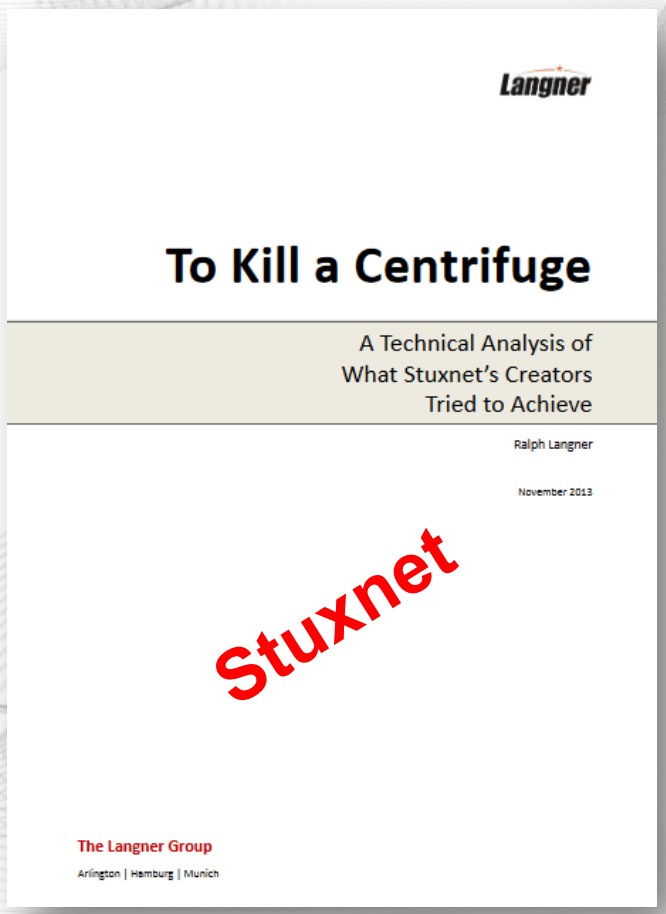
Fourth US Navy collision this year raises suspicion of cyber-attacks

by TRISTAN GREENE — 8 weeks ago in INSIDER



Finalità degli Attacchi

- Gli *attacchi* mirano a:
  - esfiltrare dati
  - rubare soldi/oggetti
  - arrecare danni
  - controllare in modo surrettizio strutture, servizi e intere nazioni
  - …


Langner
To Kill a Centrifuge
A Technical Analysis of
What Stuxnet's Creators
Tried to Achieve
Ralph Langner
November 2013
Stuxnet
The Langner Group
Arlington | Hamburg | Munich

Stuxnet

- In un articolo del The New York Times del primo giugno 2012, l'esperto di politica della Casa Bianca David E. Sanger scrive un articolo in cui anticipa la notizia che il presidente Obama abbia ordinato un cyber-attacco contro l'Iran.

- Secondo la ricostruzione di Sanger anche alcuni stati europei e alcuni ufficiali Israeliani erano coinvolti nell'operazione, l'arma utilizzata è Stuxnet:

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

From cyber to physical

- L'attacco è stato condotto con il worm Stuxnet che è passato da un sistema Windows ai controllori SCADA (*Supervisory Control And Data Acquisition*) utilizzati per il monitoraggio elettronico di una centrale nucleare iraniana.
- IL worm è riuscito a cambiare la velocità dei rotori in una centrifuga della centrale iraniana utilizzata per arricchire l'uranio.
- La compromissione è stata possibile grazie ad attività di ingegneria sociale e ad altre tecniche per non farsi scoprire (quando il rotore si era riscaldato il *malware* continuava a mandare alla centrale operativa messaggi che confermavano che era tutto ok)

Targeted Attack

- Attacco mirato e deliberato contro un target definito, sia esso un individuo, un'impresa o un sistema.

Taxonomy of Attackers (from IBM)

- Class I – *Clever Outsiders*
- Class II – *Knowledgeable Insiders*
- Class III – *Funded Organizations*

Taxonomy of Attackers (from IBM)

- Class I – *Clever Outsiders*
- Class II – *Knowledgeable Insiders*
- Class III – *Funded Organizations*

- Insufficient knowledge of system
- Not highly sophisticated equipment
- Look for existing weaknesses

Taxonomy of Attackers (from IBM)

- Class I – *Clever Outsiders*
- Class II – *Knowledgeable Insiders*
- Class III – *Funded Organizations*

- Have potential access to
  - most parts of the system
  - highly sophisticated tools

Taxonomy of Attackers (from IBM)

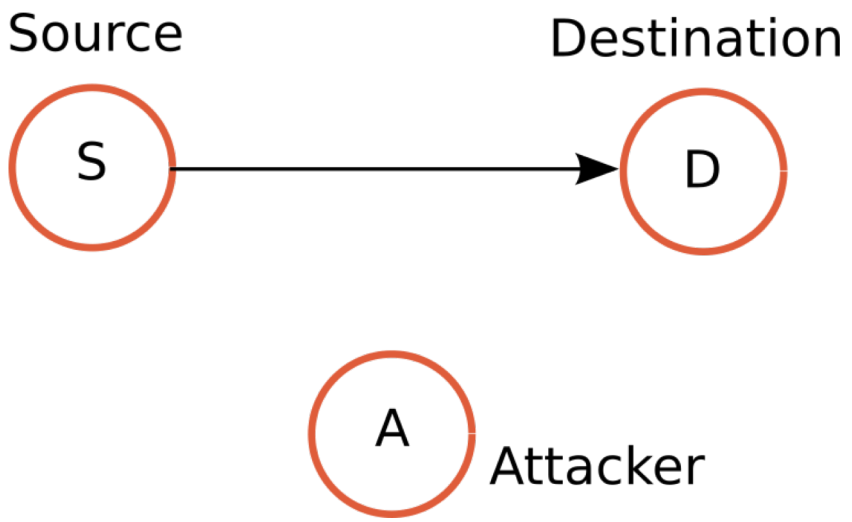
- Class I – *Clever Outsiders*
- Class II – *Knowledgeable Insiders*
- Class III – *Funded Organizations*
  - Governments, terrorists, mafia
  - They resort to
    - teams of experts
    - big budgets
    - most advanced tools

Outline

- Vulnerabilità
- Attacchi
- Classi di attacco
- Superfici di attacco
- Tipi di minaccia

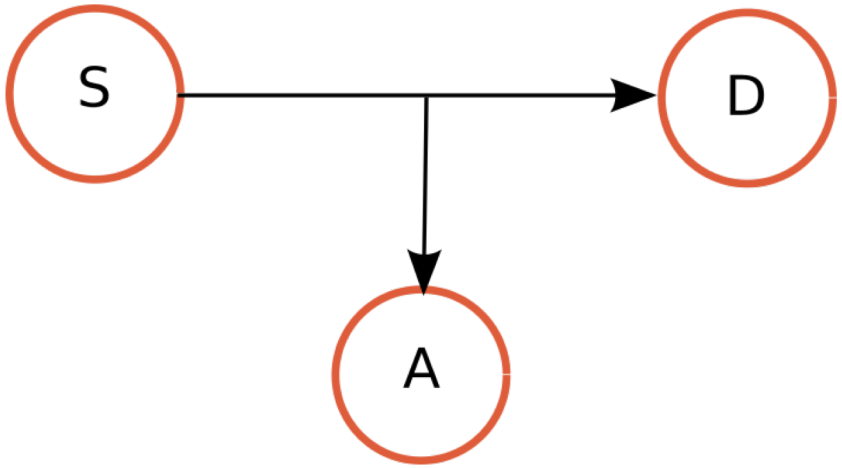
Classes of attacks

- Information (or service) flows from a source to a destination
- The attacker might **subvert** this in different ways



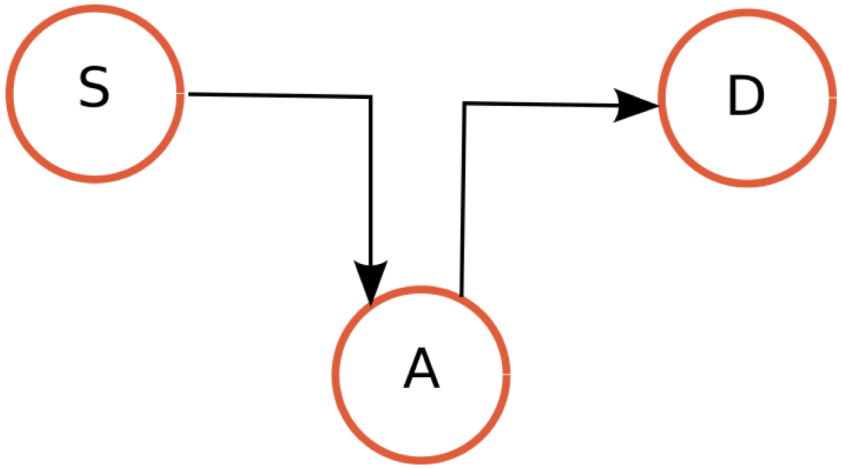
Eavesdropping

- Attacker gets **unauthorized access** to information
- Breaks **confidentiality**
- Examples:
  - S is a vulnerable database
  - S sends a credit card number to D “in the clear”



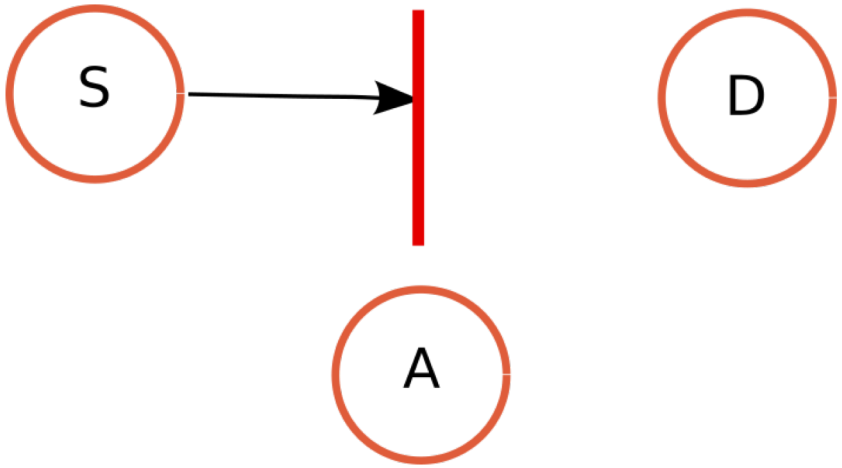
Modification

- Attacker **maliciously modifies** information
- Breaks **integrity**
- Example:
  - A redirects S's bank transfer
  - NOTE: A can be either in the browser or on the network (Man-in-the-middle)



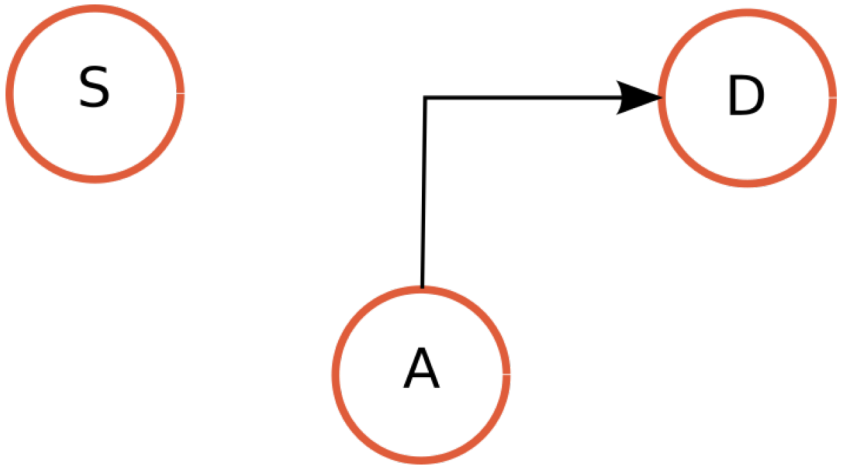
Interrupting

- Attacker **stops** the flow
- Breaks **availability**
- Examples:
  - DoS on E-Voting
  - DoS on power grid (e.g., Ukraine attacks)



Forging

- Attacker **forges new information**
- Breaks **authenticity** (and **accountability**)
- Example:
  - Forging a signature through a crypto vulnerability (e.g. MD5 collisions)



Outline

- Vulnerabilità
- Attacchi
- Classi di attacco
- Superfici di attacco
- Tipi di minaccia

- User Attacks
- Hardware Attacks
- Software Attacks
- Network Attacks
- Web Attacks

Outline

- Vulnerabilità
- Attacchi
- Classi di attacco
- Superfici di attacco
- Tipi di minaccia

Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc)
- *Cyber-espionage* (acquisizione indebita dati)
- *Cyber-terrorism* (con connotazione ideologica)
- *Cyber-warfare* (pianificazione e conduzione operazioni)

Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc)
- *Cyber-espionage* (acquisizione indebita dati)
- *Cyber-terrorism* (con connotazione ideologica)
- *Cyber-warfare* (pianificazione e conduzione operazioni)

Crime-as-a-Service

Cybercrime

- Attacking a vulnerable system is considered a **criminal act**
  - Would you enter a house just because the door is open?
- **Example**: Samy innocuous "my hero" worm took down Myspace with legal implications

Cybercrime

The 2001 Convention on Cybercrime is the first **international treaty** addressing cybercrime. It cites:

- Unauthorized access
- Unauthorized interception
- Data/system alteration
- Forgery
- Fraud
- Child pornography
- Copyright infringement

Cybercrime report

Cybercrime report

- Siamo propensi a *Cliccare qui*
- Riprendersi da un attacco informatico costa in media
  - 36 giorni
  - 114,47 US$
- Il 31% dichiara che l'attacco subito è rimasto irrisolto e senza colpevoli

Deterrenza

- Prevenzione di una azione attraverso una minaccia credibile di rappresaglia con conseguenze di dimensioni non accettabili per l'attaccante e/o attraverso operazioni che portino alla convinzione che il costo dell'azione supera i benefici percepiti.

ANALISI DELLA MINACCIA

Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc)
- *Cyber-espionage* (acquisizione indebita dati)
- *Cyber-terrorism* (con connotazione ideologica)
- *Cyber-warfare* (pianificazione e conduzione operazioni)

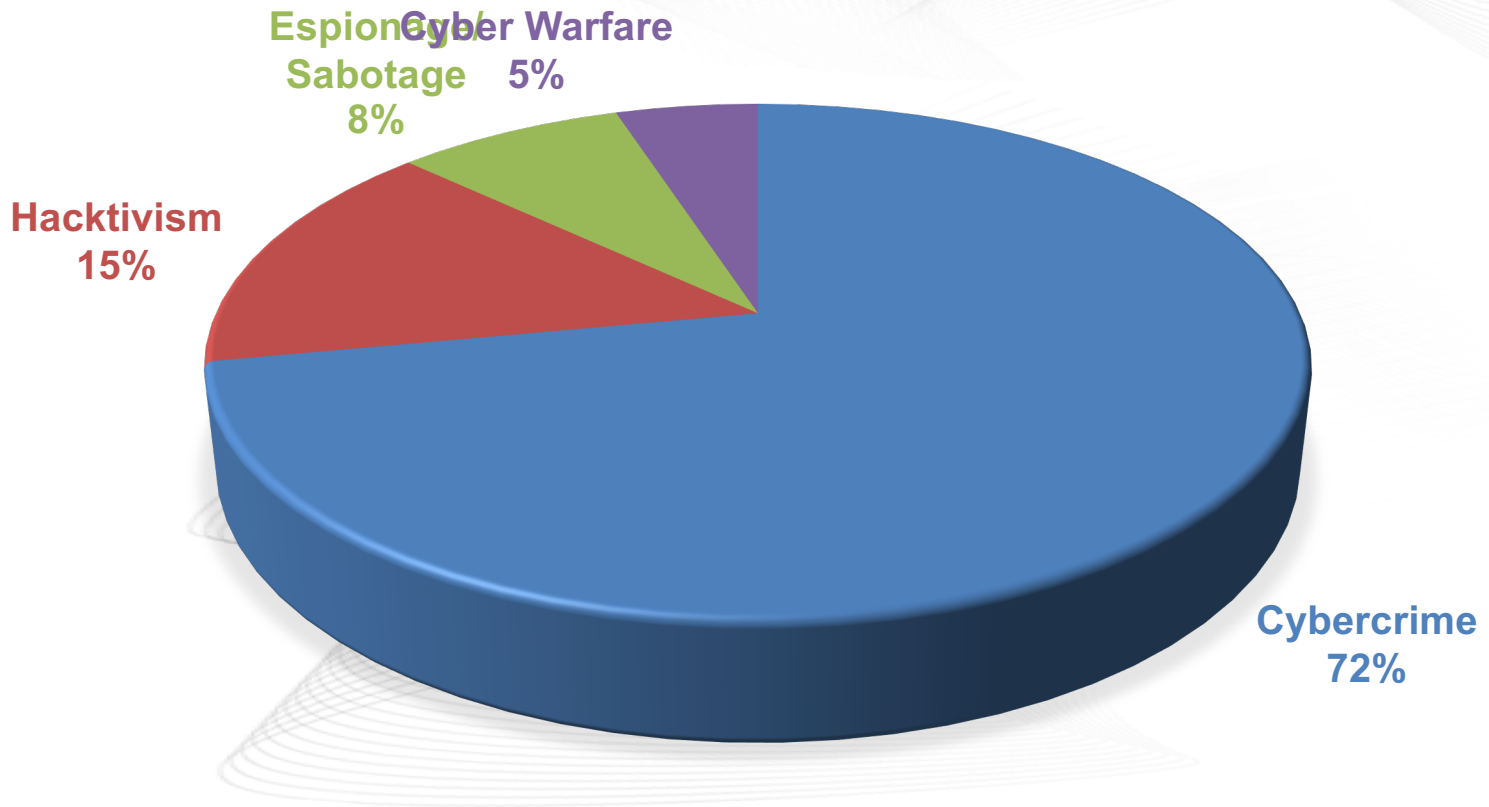
ANALISI DELLA MINACCIA

ANALISI DELLA MINACCIA

Liaoning CV 16

USS TRUMAN

TIPOLOGIA E DISTRIBUZIONE DEGLI ATTACCANTI - 2016



Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc)
- *Cyber-espionage* (acquisizione indebita dati)
- *Cyber-terrorism* (con connotazione ideologica)
- *Cyber-warfare* (pianificazione e conduzione operazioni)

CYBER-JIHAD

Tipi di minaccia

In base ad attori e finalità la minaccia si distingue in:

- *Cybercrime* (es: truffa, furto identità ecc)
- *Cyber-espionage* (acquisizione indebita dati)
- *Cyber-terrorism* (con connotazione ideologica)
- *Cyber-warfare* (pianificazione e conduzione operazioni)

CEMA (Cyber ElectroMagnetic Activities)

- Sfrutta lo spettro elettromagnetico per avere effetti cyber.
- Esempio:
  - come inoculare malware nei radar non attraverso le reti ma le onde (software defined radio)
  - gli attaccanti possono spegnere o spiare radar non con virus nei sistemi, ma tramite l'elettromagnetismo.

6 SEPTEMBER 2007: ORCHARD OPERATION

(To Alessandro Rugolo) 09/09/18 - In the 2007 in Italy we just heard of *cyber*. Someone dared to write their thesis trying to illustrate the meaning of terms like *cyberspace*, *cyberdefence*, *cyberattack*, but without proving great public success. Yet the rest of the world went on.
Israel in the meantime hit a nuclear installation in Syria with the use of the Air Force ...
The night of the 6 September at least 4 F-16I *Sufa* and 4 F-15I *Ra'am* they crossed the border with Syria towards the nuclear installation near the city of Deir ez-Zor.

The aircraft carried out their mission and all returned to the base without the Syrian anti-aircraft defenses noticing: the radars were blind and the anti-aircraft defenses did not come into operation, although they were very advanced Russian systems (Pantsir S1).
The success of the mission has always been attributed to the great skill of the Israeli pilots and to the great work of the Israeli electronic war, and yet with time the truth has emerged: the mission has succeeded thanks to the use of a cyber weapon called *Suter*.
Suter it is a computer system that, through sensors, can identify the source of electromagnetic waves, for example a radar, understand what type of transmitter it has in front of it and send signals that can confuse the transmitter or even infect it with viruses.
*Suter*according to various sources, it is an American system developed by BAE Systems and integrated on some unmanned aircraft.
There are several versions of *Suter*, the most basic allows you to understand what they see the opposing radars, the second version allows you to take control of the enemy network and control the sensors, the third version allows you to take control of sensors and actuators connected, or weapon systems . All this is achieved "simply" by injecting the ad hoc built code.

These systems are used by the US at least from the 2006 and have been deployed in Iraq, Syria and Afghanistan.

What Israel has used *Suter* or something similar created by its laboratories does not matter, what is interesting to note is that very probably for at least ten years there are technologies capable of reducing the radar to impotence.

- Non è più il mondo in cui la vulnerabilità delle reti è frutto soprattutto dell'ingenuità degli esseri umani.
- Si supera il cosiddetto air-gap per arrivare nelle reti senza entrare nelle reti stesse.
- Ci saranno aerei militari con piattaforme ISR in grado di fare a distanza tutto questo, analizzando le informazioni che passano via Wi-Fi

[**Francesco Vestito -** comandante del CIOC - Comando Interforze per le Operazioni Cibernetiche]

CYBER COME FORMA DI GUERRA "IBRIDA"

Guerra Ibrida: nuova tipologia di guerra complessa che impiega un uso centralizzato, controllato e combinato di tattiche nascoste e non (tra cui *cyber attack*)

***Cyber attack*:**

- ✓ favorevole rapporto costo/efficacia;
- ✓ "sotto la soglia" della reazione militare;
- ✓ assenza di confini geografici e difficoltà attribuzione.

State-sponsored cyberattacks

The Rise of Global State-Attributed Cyberattacks
2005-2018

Each attack is marked as a diamond, sized by the number of targets. Attacks can have both state and non-state targets; where state targets are indicated, lines are drawn to those countries.

source: Council on Foreign Relations

Titan Rain
August 2005

Titan Rain was a string of cyber operations that compromised a number of agencies within the US and UK government. Although the attacks were first publicly revealed in 2005, the United States reported that they had been ongoing since at least 2003.

Ghostnet
March 2009

A large-scale electronic espionage program used to spy on individuals, organizations and governments, breaching 1,295 computers in 103 countries over a two-year period, predominately focusing on governments in South-East Asia.

Shady RAT
August 2011

Targeted government entities (primarily in the United States), defence contractors, think tanks, and companies in the advanced information technology and aero-space industries for espionage.

Flame
May 2012

A threat actor, using a tool called Flame, targeted computers in the Middle East region; the most compromises were in Iran. This compromise gained widespread coverage due to the modular nature of the malware the threat actors used.

Machete
August 2014

This threat actor targets military, government entities and telecom-munications providers, primarily in Latin America, for the purpose of espionage.

Operation Parliament
April 2018

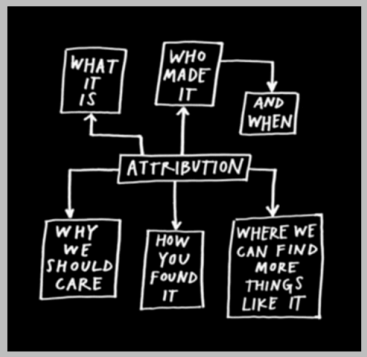
A threat actor targeted a foreign ministry in Europe and in North America using spear-phishing techniques for the purpose of espionage.

The issue of attribution

- "Most sophisticated and exhaustive approaches to attribution are often outside the means of most companies, and from the perspective of the government or its intelligence organizations, is usually classified or sensitive."

2017 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

PHASE II - CYBER ATTRIBUTION USING UNCLASSIFIED DATA

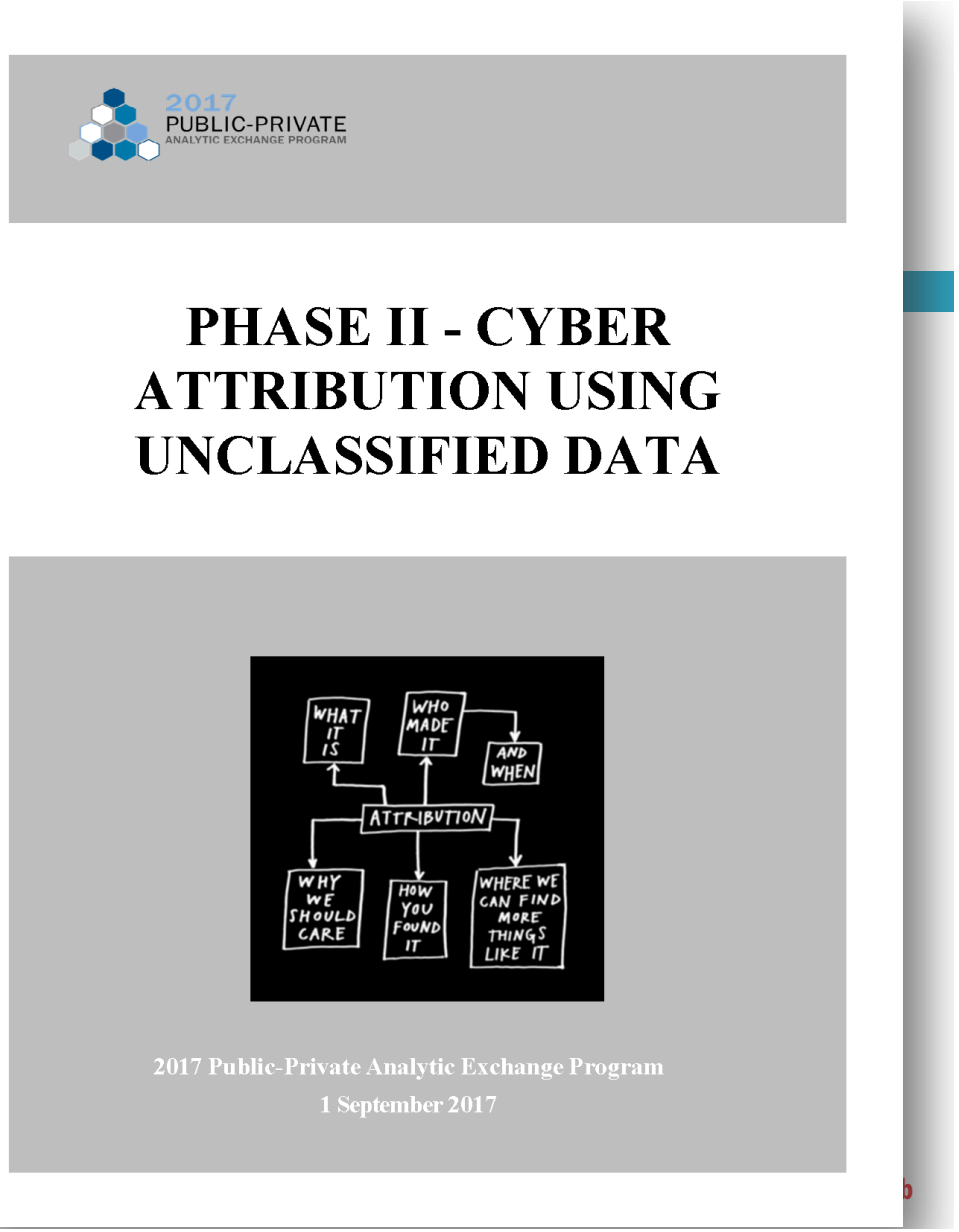


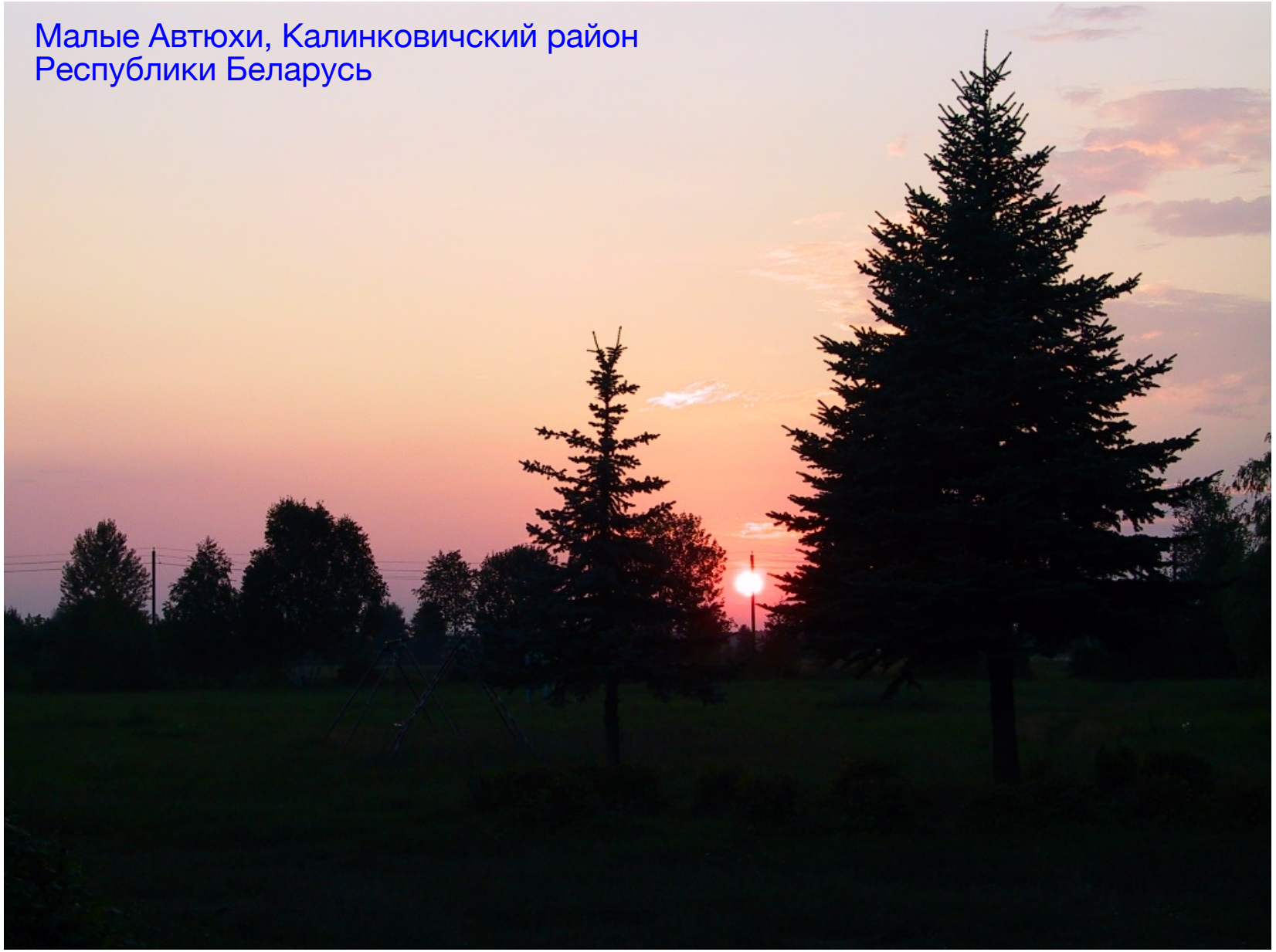
2017 Public-Private Analytic Exchange Program

1 September 2017

The issue of attribution

- This leaves private enterprise in a difficult position when it is targeted by state actors. They may fail to anticipate being targeted and lack the ability to respond when they are.





Paolo PRINETTO
Director
CINI Cybersecurity National Laboratory
Paolo.Prinetto@polito.it
Mob. +39 335 227529

cini
Cybersecurity
National Lab

www.consorzio-cini.it