Attacchi

Goal

- Presentare una tassonomia dei principali attacchi alla cybersecurity e una breve rassegna di alcuni attacchi particolarmente significativi

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

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

Attacco

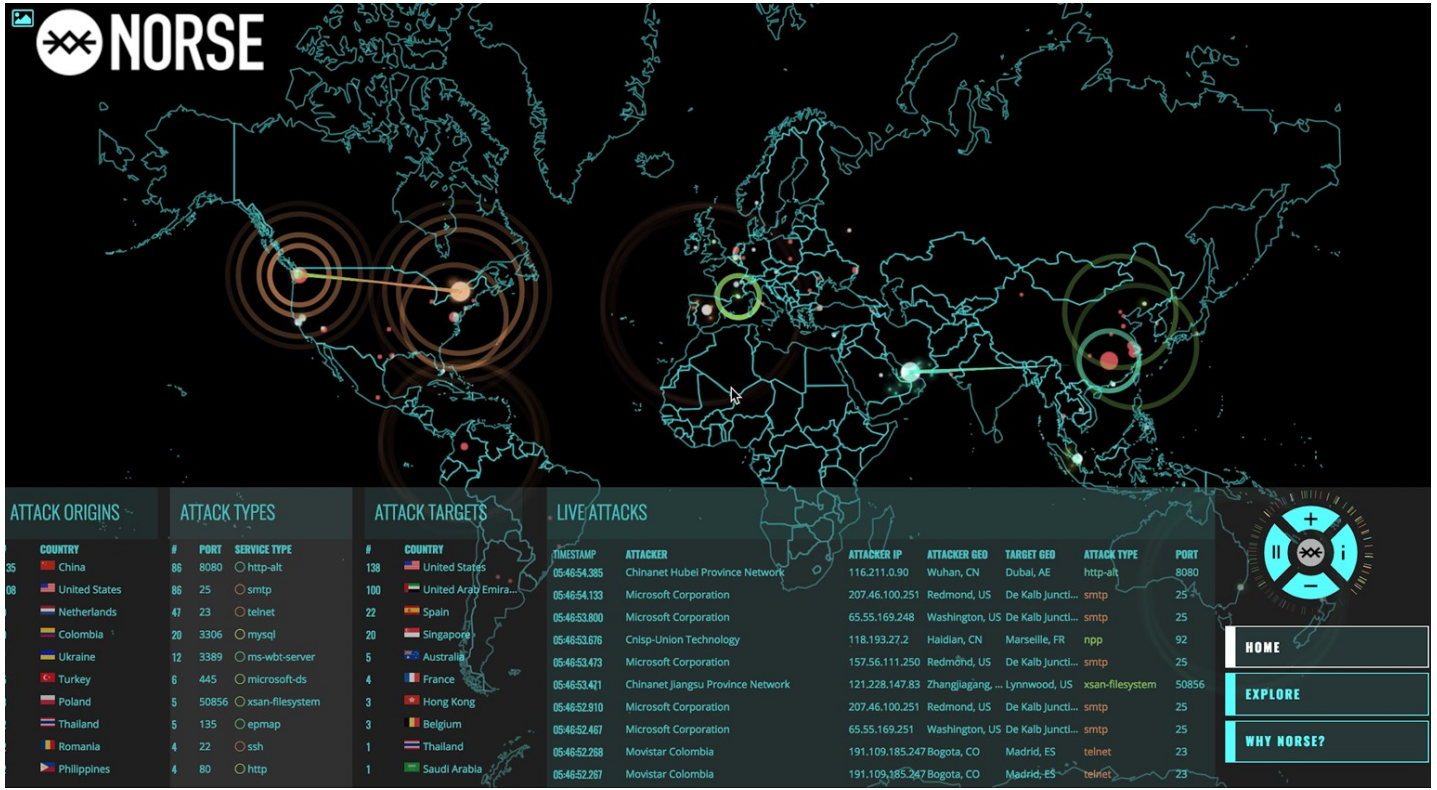
- Qualsiasi tipo di attività dannosa che tenta di raccogliere, interrompere, negare, degradare o distruggere le risorse del sistema informativo o le informazioni in esso contenute.

[RFC 2828, Internet Security Glossary, May 2000]

Tutto è sotto attacco

… sempre …

http://map.norsecorp.com/#/



Finalità degli Attacchi

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

Finalità degli Attacchi

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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)

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

Finalità degli Attacchi

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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)

Cybercrimine

Definito come tale per la prima volta dalla Convenzione del Consiglio d'Europa sulla Criminalità Informatica, siglata a Budapest il 23.11.2001.

[https://www.poliziadistato.it/statics/14/convenzione-cybercrime.pdf]

Convenzione di Budapest

- Afferma che la criminalità informatica comprende:
  - Accesso non autorizzato
  - Intercettazioni non autorizzate
  - Alterazione di dati e sistemi
  - Contraffazione
  - Frode
  - Pedopornografia
  - Violazione del copyright
  - …

Caveat

- Attaccare un sistema vulnerabile è considerato un atto criminale:
  - Entreresti in una casa solo perché la porta è aperta?

Cyberspace: terra di nessuno…

- Nel cyberspace i paradigmi sociali sono radicalmente diversi
- Il cyberspace è spesso considerato *terra di nessuno* a causa di
  - assenza di confini evidenti
  - mancanza di una chiara giurisdizione transnazionale

Conseguenze (1)

- Grande asimmetria tra attaccanti e difensori (a favore degli attaccanti)

Conseguenze (1)

- Grande asimmetria tra attaccanti e difensori (*a favore degli attaccanti*)

- Gli aggressori tendono a condividere le informazioni
- I difensori tendono a nasconderle e a mantenere il silenzio

Conseguenze (2)

- Continuo incremento del rapporto *costi/benefici* per l'attaccante:
  - per lui è sempre più facile raggiungere il bersaglio desiderato, indipendentemente dalle rispettive localizzazioni geografiche

Conseguenze (3)

- Criminali e terroristi sono in grado di arrecare sempre più danni con:
  - pochissimo sforzo
  - relativamente basso rischio
  - scarse conoscenze tecnologiche
- *Crime-as-a-Service*

Conseguenze (4)

- Molti nuovi modi per :
  - Commettere crimini
  - Sferrare attacchi
  - Arrecare danni
  - Combattere guerre
  - Perpetrare atti ostili
  - …

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

Cybercrime: Esempi

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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)

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

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

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

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

Cybercrime: Esempi

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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)

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)

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

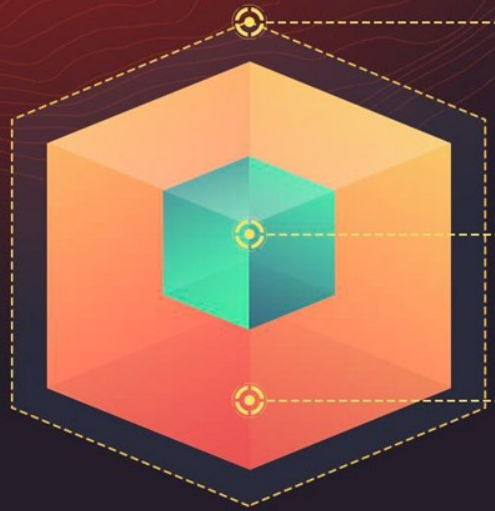
Infecting bank clerks' computers

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]

Two cases of cyber-attacks in the financial sector

1. SWIFT Systems

2. Carbanak APT

(*Advanced Persistent Threats*)

SWIFT Systems: What happened?

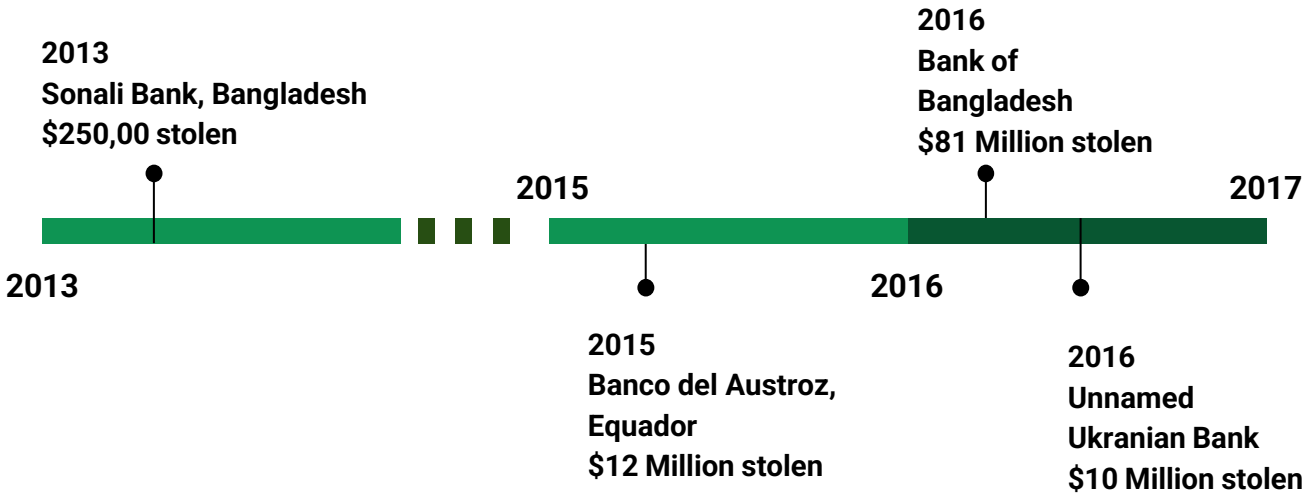
- **At least 8 high-profile attacks on SWIFT Systems in 2013-2017**
- **Collective theft of around $167,210,000**.
- Affected institutions of **all sizes and levels of security maturitv**.

1. Attackers deploy malware to access the bank internal network

2. Laterally moves across the network in search of SWIFT connected systems

3. Attackers compromise SWIFT operator credentials and use SWIFT software to issue fraudulent transactions

Timeline: High-profile SWIFT-related attacks

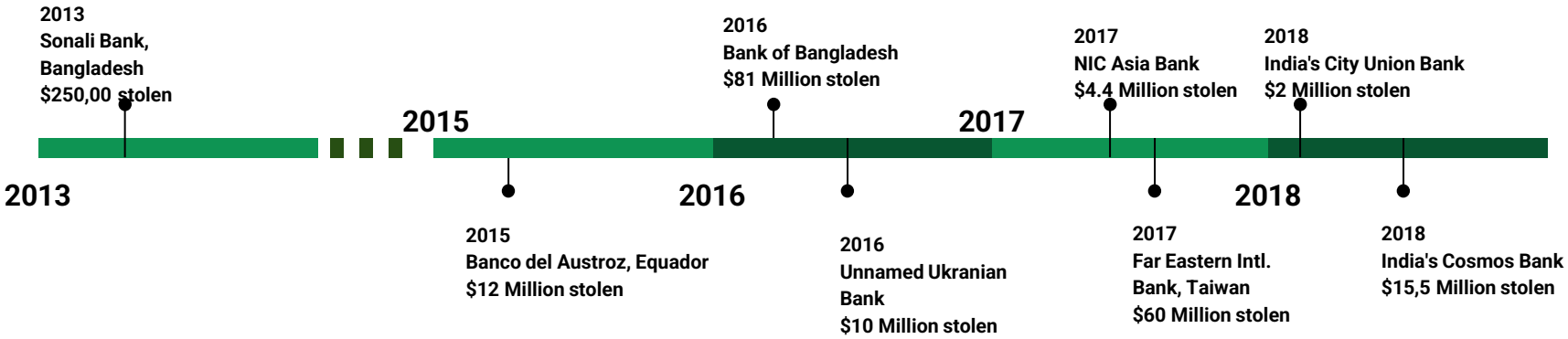


Lessons Learnt

- “This attacker put significant effort into
  - **deleting evidence of their activities**,
  - **subverting normal business processes to remain undetected** and
  - **hampering the response from the victim**.
- The wider lesson learned here may be that **criminals are conducting more and more sophisticated attacks against victim organisations** [...].
- As the threat evolves, **businesses and other network owners need to ensure they are prepared to keep up with the evolving challenge of securing critical systems**.”

\- *BAE Systems Threat Research Blog*

Lessons Learnt?!?



CARBANAK / COBALT

- **Carbanak cybercrime group** is suspected of stealing **$1 billion from financial organisations** since its early attacks in 2013
- More than 100 financial institutions targeted in at least 40 countries

...some findings

- **Gangs do not necessarily have prior knowledge of the inner workings of targeted organizations**.
- To understand how a institution operates, **infected computers were used to conduct surveillance on usual activity and then replicate it.**

Lessons Learnt

- Carbanak campaign is a clear indicator of a new era in cybercrime in which criminals **use Advanced Persistent Threat (APT) techniques against the financial industry**.
- **APTs are not only for stealing information anymore.**

Attacks against the Supply Chain

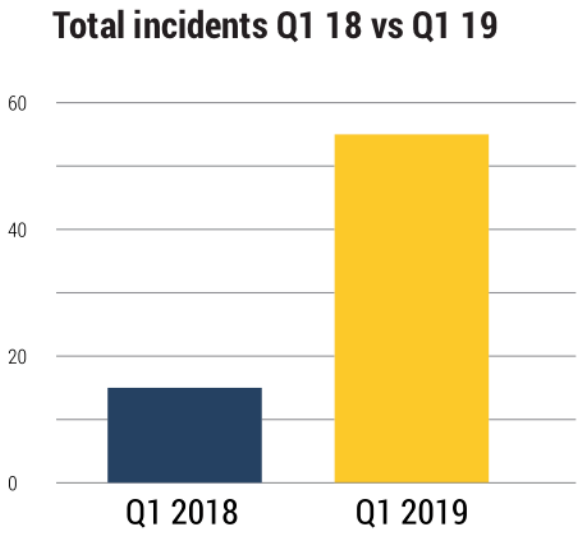
- In Feb 2017 attacked four **IT integrators** and used them as a vehicles to conduct attacks on their customers.
- In March 2017 Cobalt infiltrated a **company providing electronic wallets and payment terminals**. Eight companies in Russia and Ukraine attacked with more than USD 2 million transferred.
- In Sep 2017, Cobalt (in liason with Carbanak group) attacked a company which produces **software for payment terminals**.

Crime-as-a-Service

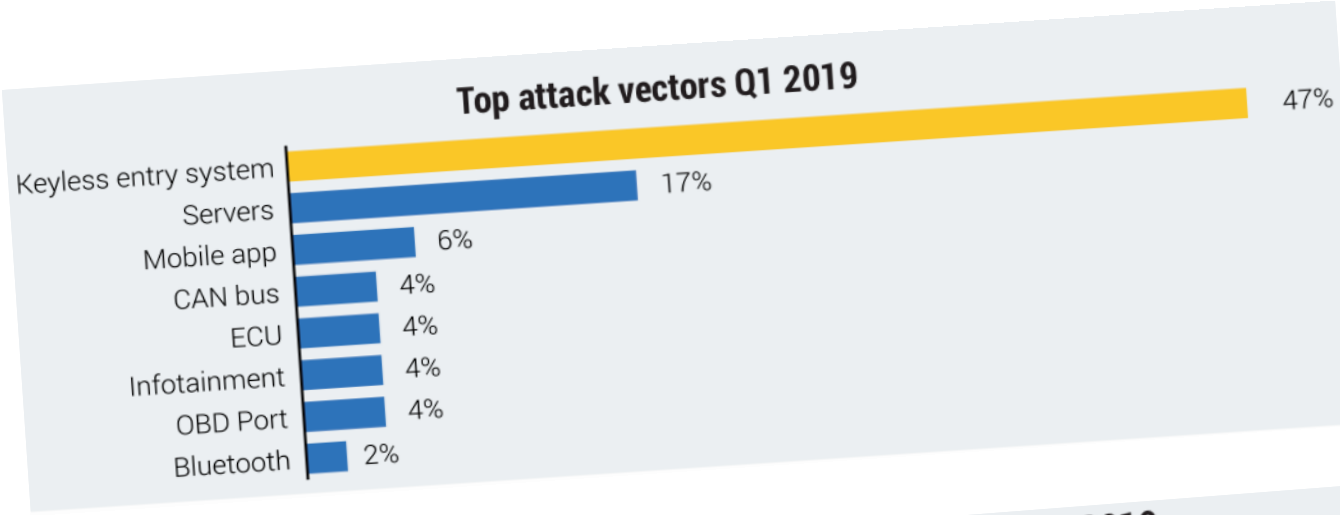
Automotive attacks

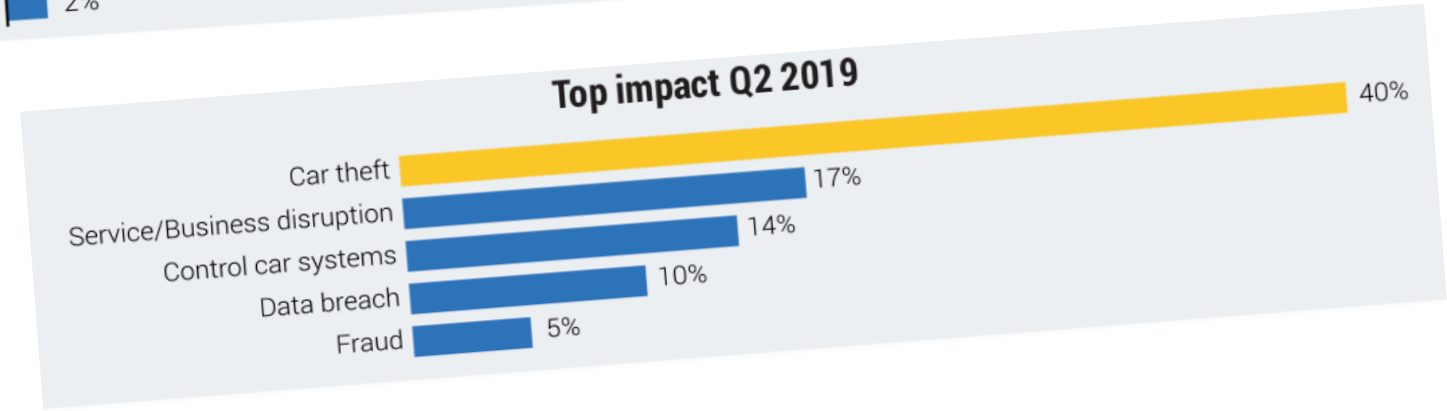
Upstream

Q1 2019 SEES RAPID GROWTH OF AUTOMOTIVE CYBER INCIDENTS



Automotive attacks





Cybercrime: Esempi

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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)

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.

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 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 t 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

Ascolta

LA COMUNICAZIONE

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

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

Cybercrime Costi - 2017

CYBERSECURITY

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GU

Cybercrime costs the global economy $450 billion

Luke Graham | @LukeWGraham

Published 10:00 AM ET Tue, 7 Feb 2017

CNBC

Austria GDP (Gross Domestic Product) in 2017: $434 billion

Cybercrime vs. space

GLOBAL SPACE BUDGET:

$33 BILLION

[E. Kaspersky, 2018]

Cybercrime vs. space

Cybercrime Costi - 2020

Il cybercrime è la terza potenza economica mondiale

Cybercrime Costi - 2020

Arturo Di Corinto

EDIZIONE DEL
16.04.2020

PUBBLICATO
15.4.2020, 23:59

Secondo l'ultimo rapporto del World Economic Forum sui rischi globali le attività degli hacker si stanno industrializzando, e per il 2021 i danni causati dai cybercriminali potrebbero arrivare a 6 trilioni di dollari, l'equivalente del prodotto interno lordo della terza economia mondiale. Per capirci Tesla, Walmart, Facebook, Microsoft, Apple, Amazon messi insieme non arrivano a un trilione e mezzo di ricavi.

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

Cyber-espionage

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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-espionage ??

Cyber-espionage ??

Liaoning CV 16

USS TRUMAN

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

Cyber-terrorism

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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


HAYA ALAL
JIHAD
TILL THE DAY OF JUDGMENT
NASHEED
RISE UP!
(LET'S GO FOR JIHAD!)

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

Cyber-warfare

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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)

Il IV dominio

- Nel 2016, durante il summit di Varsavia, la NATO ha ufficialmente elevato il *cyberspace* al rango di "*dominio delle operazioni*" insieme a *terra*, *mare* e *aria*.

CEMA (Cyber ElectroMagnetic Activities)

- Sfrutta lo spettro elettromagnetico
- Esempi:
  - vengono inoculati dei malware nei radar sfruttando le onde e non la rete dati.
  - gli attaccanti possono spegnere o spiare radar non iniettando virus nei sistemi, ma attraverso l'elettromagnetismo.

Cyber-warfare: Esempi

Gli *attacchi* mirano a:

- Rubare:
  - Dati:
    - Personali, Aziendali, Statali
  - Soldi
  - Oggetti
  - Identità
  - Ruoli
- Arrecare danni
- Controllare in modo surrettizio:
  - Strutture
  - servizi
  - intere nazioni

- 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)

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.

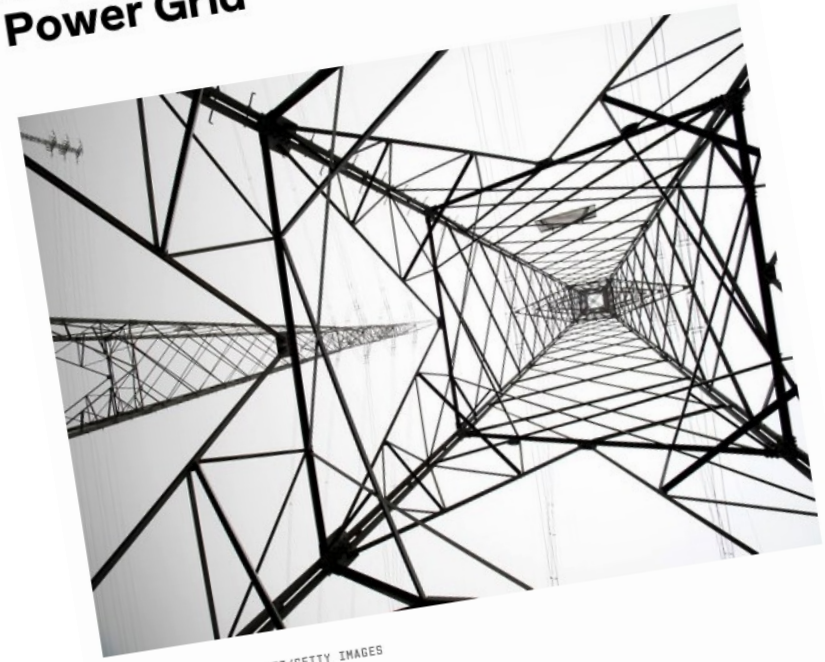
The aircraft carried out their mission and all returned to the base without the Syrian anti-aircraft defenses noticing: the radars were blind and the anti-aircraft defenses did not come into operation, although they were very advanced Russian systems (Pantsir S1).
The success of the mission has always 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.

2015, Dec. 23rd

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid



JOSE A. BERNAT BACET/GETTY IMAGES

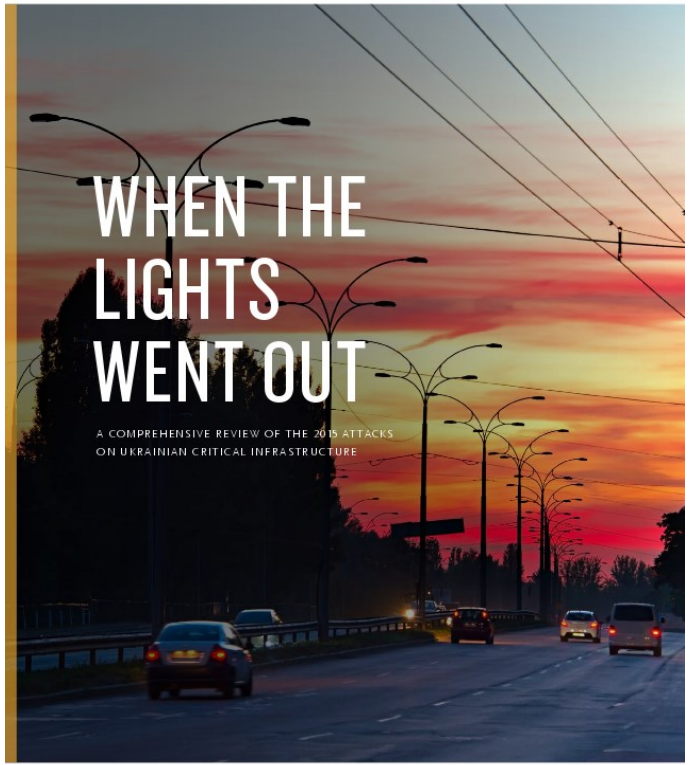
IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their

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.

Booz | Allen | Hamilton



CONSULTING | ANALYTICS | SYSTEMS DELIVERY | ENGINEERING | CYBER

SANS ICS Industrial Control Systems

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

March 18, 2016

1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com

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

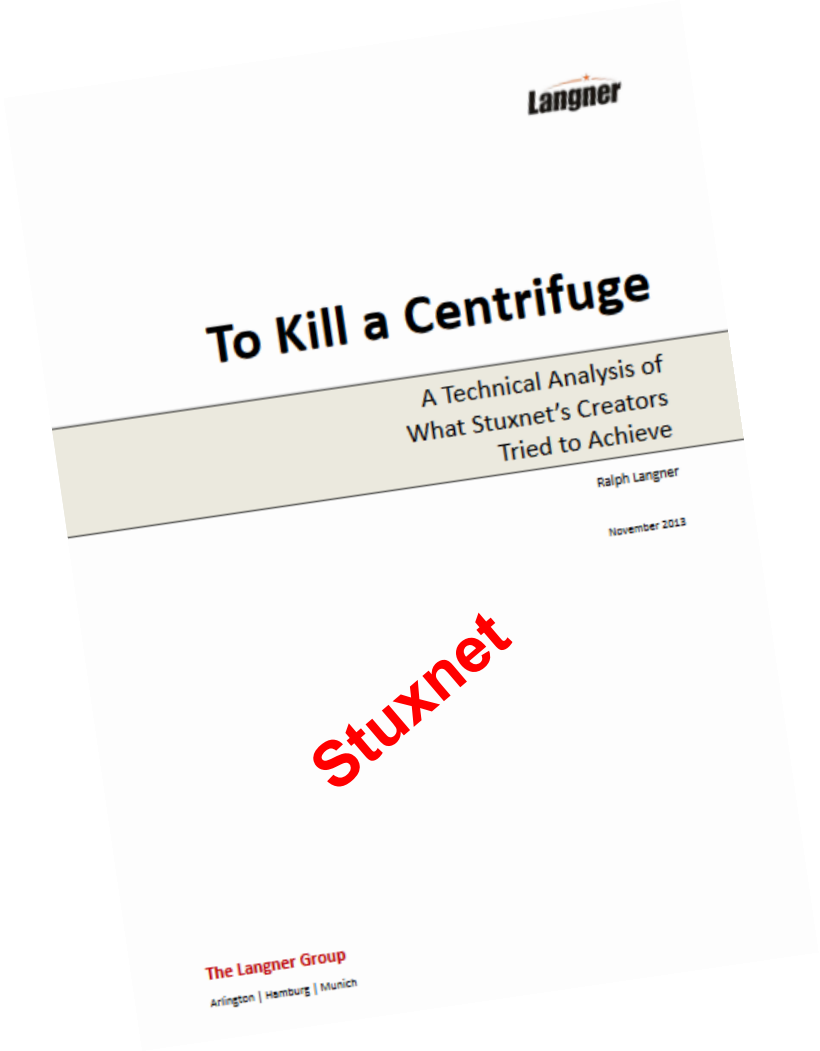
Il tanto temuto blackout provocato da attacco informatico alle centrali elettriche è arrivato. Il primo vero salto di qualità nelle minacce hacker ad impianti elettrici è avvenuto il 23 dicembre scorso, ai danni della rete elettrica ucraina nel Nord-Ovest del Paese: lo ha reso noto l'azienda di sicurezza 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.

Stuxnet


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]

Dal cyberspazio al dominio fisico

- 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 malware 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)

Trump secretly ordered cyber attacks against Iran missile systems

June 23, 2019 By Pierluigi Paganini

The United States launched a series of cyber attacks on Iran after the Iranian military has downed an American surveillance drone.

The military response to Iran, after the Iranian army has downed an American surveillance drone, started from the cyberspace.

US President Donald Trump first approved military strikes against Iran in retaliation for downing a surveillance drone, but pulled back from launching them on Thursday night after a day of escalating tensions.

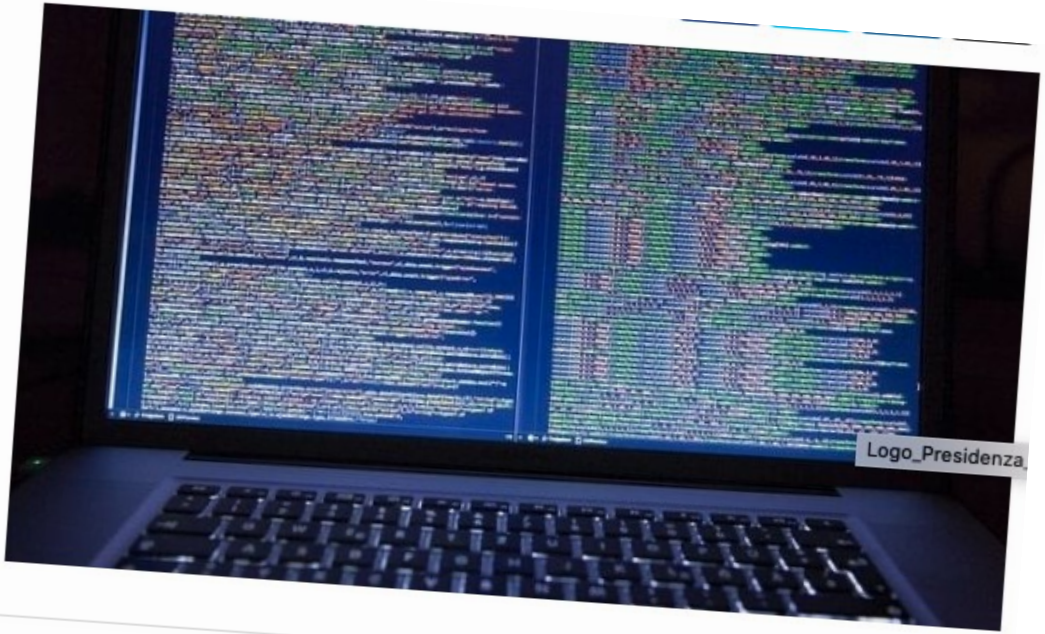
Report: US Cyberattack Crippled Iran's Ability to Target Oil Tankers

The June 20 cyberattack, carried out in response to Iran's downing of a US drone, took out an Iranian database used by the IRGC to plan attacks against oil tankers in the Gulf, the New York Times reported

IsraelDefense | 29/08/2019

A speedboat of the Iran's Revolutionary Guard moves around a British-flagged oil tanker Stena Impero, which was seized in the Iranian port of Bandar Abbas (Hasan Shirvani/Mizan News Agency via AP)

Israele vs Iran: il nuovo fronte di guerra è il cyberspazio



Un attacco hacker ha bloccato il porto di Shahid Rajaee sul Golfo Persico pochi giorno dopo l'incursione informatica nel sistema idrico israeliano. Gli esperti: è l'alba di un nuovo tipo di conflitto, senza regole

20 maggio 2020

State-sponsored cyberattacks

Guerra Ibrida

- *Hybrid warfare* is a military strategy which employs political warfare and blends conventional warfare, irregular warfare and *cyberwarfare* with other influencing methods, such as fake news, diplomacy, lawfare and foreign electoral intervention.

Guerra Ibrida

- La *guerra ibrida* è una strategia militare che impiega la guerra politica e fonde la guerra convenzionale, la guerra irregolare e la guerra cibernetica con altri strumenti di influenza, quali le notizie false, la diplomazia e gli interventi durante le campagne elettorali.

Attacchi Cyber nella Guerra Ibrida

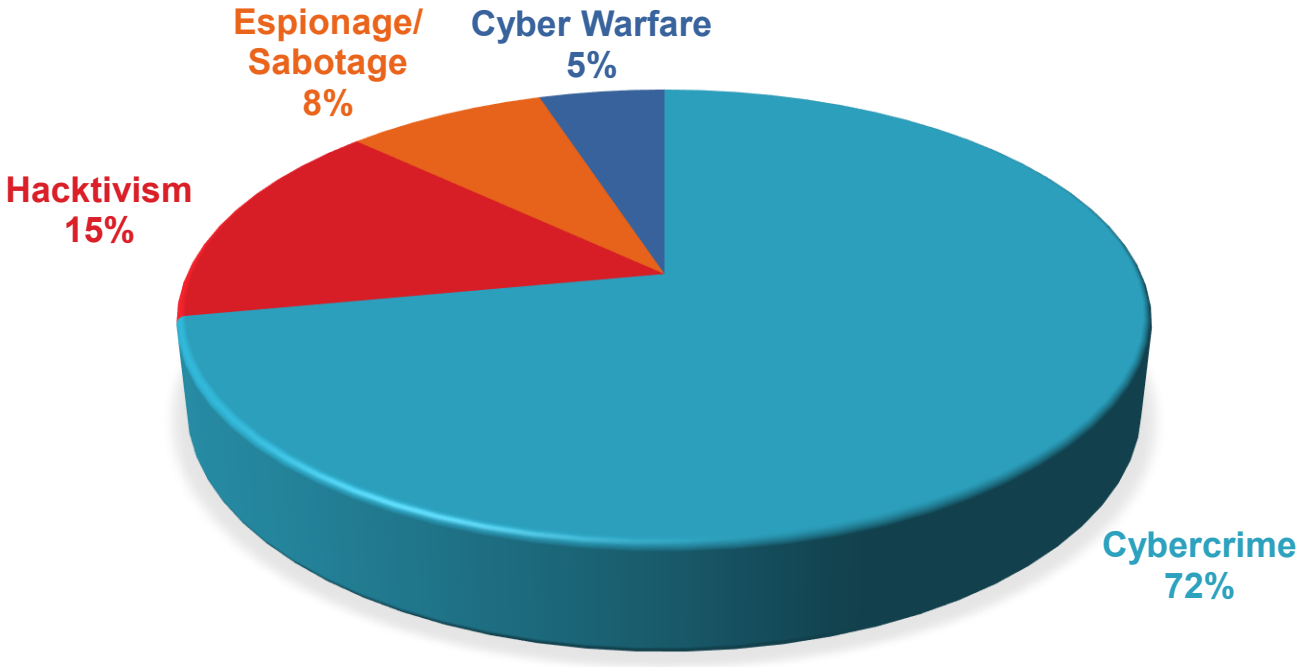
- Why Cyber attacks in *Hybrid warfares*:
  - Costi-benefici
  - Rimangono spesso “sotto la soglia” rispetto a una reazione militare
  - Difficoltà nell’attribuzione

Outline

- Attacchi
- Cybercrime:
  - Motivazioni
  - Esempi
  - Costi
- Cyber-espionage
- Cyber-terrorism
- Cyber-warfare
- Conclusioni

THREAT ANALYSIS

TYPES AND DISTRIBUTION OF ATTACKERS - 2016



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