Cyber(in)security

google “alberto bartoli trieste”

Obbiettivo 1:
Capire che il mondo è cambiato

- **Non** è una "**moda transitoria**"
- **Non** è un problema "**da informatici**"
- **Non** è un problema "**da tecnici**"

Obbiettivo 2:
Suggerimenti pratici

- Uso "il più possibile sicuro" dei dispositivi
  - Personali
  - Lavoro

- "Pochi e focalizzati"
  1. Email
  2. Password

Struttura

- Parte 1:
  - Sensibilizzazione
  - Comprensione

(pausa)

- Parte 2:
  - Suggerimenti pratici (**pochi** e **focalizzati**)

Parte 1-a:

Sensibilizzazione

Problema reale
Problema pervasivo (nessuno è immune)

Evento MOLTO significativo (Febbraio 2016)

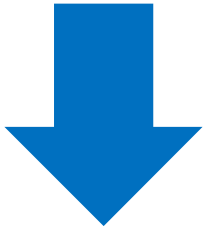
Clever bank hack allowed crooks to make unlimited ATM withdrawals

Banking malware is using techniques once reserved for state-sponsored hacking gangs.

- Malware nei PC interni alla Banca
- **Cancella** evidenza prelievo al Bancomat (+ prelievi **illimitati**)
- Malware sofisticatissimo (30 moduli)

Perché MOLTO significativo?

- Attacchi hanno **forti motivazioni**
  - Tipicamente economiche (ma non sempre)
- Sono attività **professionali**



1. Grande **sofisticazione** tecnica
2. DilettantiDistratti vs ProfessionistiFocused

Atteggiamento comune (SBAGLIATISSIMO)

- *"Vabbè, si sa che attaccano le banche"*

Non è vero:
Dipende solo dalla convenienza

- **Innumerevoli** esempi per:
  1. Guadagnare da attacchi
     (non solo **finanziario** e **diretto**)
  2. Con Costo Attacco < Guadagno

- **Non ce ne rendiamo conto**

- Seguono esempi

Password (November 2019)

Thousands of hacked Disney+ accounts are already for sale on hacking forums

- Many of these accounts are now being **offered for free** on hacking forums, or available **for sale** for prices varying from $3 to $11

Internet Banking Credentials: (April 2016)

Underground Hacker Markets

ANNUAL REPORT—APRIL 2016

SecureWorks

Bank Account Credentials	Price based on account balance
Bank accounts — ANZ (Australia)	$18,000 cost $4,750
Bank accounts — ANZ (Australia)	$22,000 cost $2,250
Bank accounts — ANZ (Australia)	$62,567 cost $3,800
Bank accounts with no balance listed — Turkey, Sweden, Norway, Romania, Bulgaria, Croatia,	$400 (flat fee)
Bank accounts — (U.K.)	$27,003 cost $2,000
Bank account — (U.S.)	$1,000 cost $40
Bank account — (U.S.)	$2,000 cost $80
High Quality Bank Accounts with Verified, Large Balances of $70,000 – $150,000	6% of the balance of the account

Segreti industriali (Luglio 2019)

Mitsubishi Electric Hacked nippon.com

Jan 20, 2020

- Following a months-long investigation, Mitsubishi said...they stole roughly **200 MB of files**.
- Files with corporate confidential technical materials, sales materials, and others.

ZDNet

Credit and financial data (Settembre 2017)

Stand up who HASN'T been hit in the Equifax mega-hack – whoa, whoa, sit down everyone

The Register

7 Sep 2017

143m in US, unknown number in UK, Canada – gulp!

- ...massive breach of security that could affect **almost half of the US population**.

- ... hackers managed to get access to some of its internal data in **mid-May**... They remained on the system until they were discovered on **July 29**.

Personal Info (November 2018)

Marriott reveals massive database breach affecting up to 500 million hotel guests

The Verge

Nov 30, 2018,

- ...unauthorized access to the Starwood network since **2014**...
- **327 million** records of “personal info”
- Unknown number of payment information

De novo! (July 2022)

The Marriott hotel chain has been hit by another data breach

Jul 6. 2022

- ... around 20GB of data, including **confidential business documents** and **customer payment information**...

Impronte digitali (Settembre 2015)

Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says

The New York Times

- The hackers got the fingerprints of **5.6 million** federal employees
- Biometric authentication? Una password può essere revocata...un fingerprint no
- Potenziale per **ricatti** enorme

Cartelle sanitarie (Stati Uniti 2015)

Data Breaches In Healthcare Totaled Over 112 Million Records In 2015

Forbes

- 112 milioni di file (35% popolazione US)
- 6 furti > 1.000.000
- 253 furti > 500

Cartelle sanitarie (Norvegia 2018)

'Professional' hack on Norwegian health authority compromises data of three million patients

the INQUIRER

Local security centre blames breach on 'advanced' hackers

18 January 2018

- Letteralmente mezza Norvegia...

Takeaway

- Rubare informazioni è **relativamente semplice**
  - Anche su **larga** scala
  - Anche a entità **molto** protette

- **Molti** modi per estrarne valore
  - Non necessariamente "finanziario diretto"

E i "nostri dispositivi"?

- **Innumerevoli** esempi per:
  1. Guadagnare da attacchi
     (non solo **finanziario** e **diretto**)
  2. Con Costo Attacco < Guadagno

- Idem

1. Permettono guadagno agli attaccanti
2. Prenderne possesso è "cost-effective"

Esempio importante: Botnet

- Bot
  - **Malware** controllabile da **remoto**
  - **Invisibile**

- **Botnet**
  - **Insieme** di bot controllati da **un** bot master
  - Ne esistono **molte**
  - Di solito **centinaia di migliaia** di bot

https://reti2.blogspot.it/search?q=botnet
https://news-bartolialberto.blogspot.it/search?q=botnet

Premessa: Pubblicità sul web

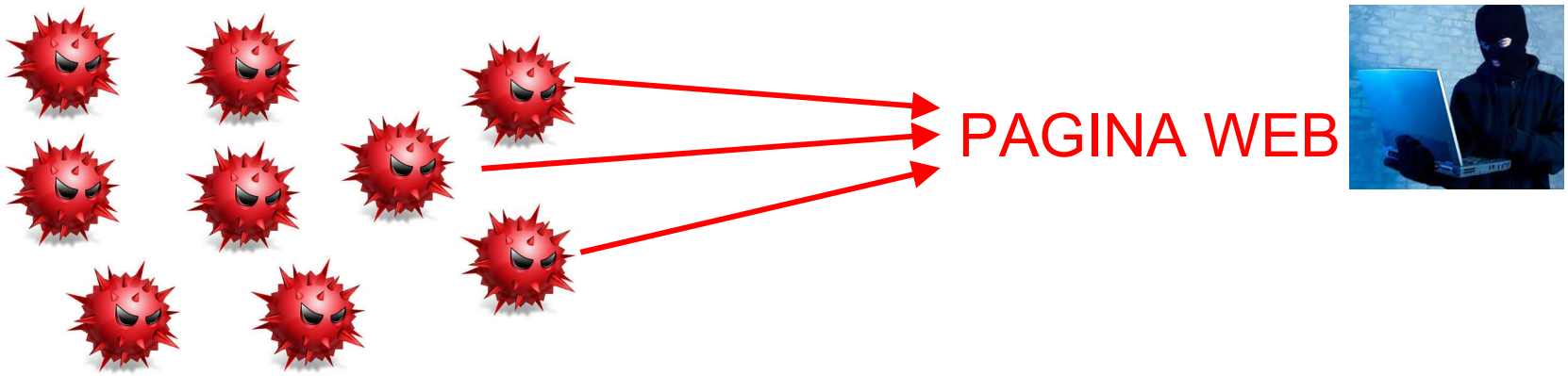
PAGINA CHE RICEVE $$$ in proporzione al numero di view/click

INSERZIONISTA

Botnet application: Clickfraud

- Attacker:
  - Crea sito web
  - Sottoscrive contratto con "ad broker"
  - Istruisce migliaia di bot a:
    1. Prelevare il proprio sito web
    2. Cliccare sulle pubblicità
  - Incassa per pubblicità che **nessuno vede**
  - Utente di ogni bot non si accorge di **nulla**

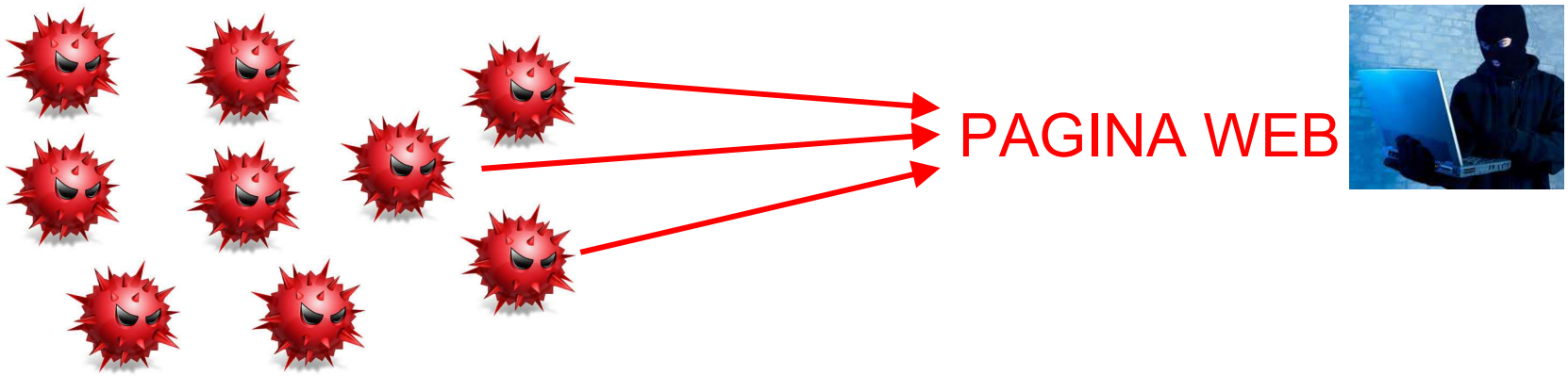
Botnet: ZeroAccess (2012)



- Botnet ZeroAccess ha generato circa un milione di click fraudolenti al giorno
- ...equivalgono a circa **$100,000 al giorno**

https://reti2.blogspot.it/search?q=clickfraud

Botnet: 3ve (2018)



- 700K bot ogni giorno su 10k siti web
- +3 miliardi di click fraudolenti al giorno

- ...equivalgono a **non-mi-ci-fate-pensare**

google "the hunt for 3ve"

Botnet application: Riuso Credenziali

How Hackers Become You With Credential Stuffing

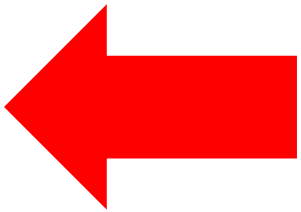
Forbes

1. Furto migliaia username-password da un sito
2. Bot master le ottiene e **distribuisce ai bot**
3. **Ogni bot** prova ad usarle su **molti altri siti**

   Automaticamente e lentamente...

Si possono affittare i bot

- Il Bot Master può **affittare** i bot
  - Acquirente ci installa il malware che vuole
- Costo unitario **decine di centesimi** (!)



- 1000 bot:
  - Asia $13
  - Europe $35
  - US $125

https://reti2.blogspot.it/2016/05/crime-report-2016.html

Un nuovo (TERRIBILE) business model: Ransomware

- Dati e Sistemi resi **inutilizzabili** fino al pagamento di un **riscatto** ("**ransom**")

e/o

- Minaccia **pubblicazione** dati se non viene pagato riscatto

- Monetizzazione **diretta!**
  - **Ogni** bersaglio ha valore
- Enormemente facilitato da **bitcoin**
  - Globale + Anonimo

Servizio Sanitario Irlanda (May-September 2021)

HSE cyber-attack: Irish health service still recovering months after hack

BBC 5 September 2021

- The attack in **May** was unprecedented in the history of the Irish state, affecting almost every part of its healthcare system, already worn down by more than a year of fighting Covid-19.
- The staff reverted to a paper system and the number of appointments in some areas dropped by 80%

google "Conti attack HSE full report"

L'amministrazione di una città intera! (Maggio 2019)

Hackers have been holding the city of Baltimore's computers hostage for 2 weeks

recode

- **Tutte** le operazioni informatiche **bloccate** (ad eccezione di polizia e pompieri)
- Più di **due settimane**

Fabbricante di alluminio - NORSK HYDRO (Marzo 2019)

MOTHERBOARD | By Lorenzo Franceschi-Bicchierai | Mar 19 2019, 5:33pm
TECH BY VICE

Ransomware Forces Aluminum Manufacturing Giant to Shut Down Network Worldwide

- Uno dei più grandi al mondo: 35.000 dipendenti in 40 paesi
- Ha dovuto **spegnere** la rete **in tutto il mondo (160 impianti)**: produzione e uffici

- Danni stimati 50$ milioni

Spedizioni marittime - MAERSK (Estate 2017)

Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack

BLEEPINGCOMPUTER January 25, 2018

- Il più grande armatore di navi mercantili del mondo
- Ha dovuto reinstallare **4,000 servers**, **45,000 PCs**, e **2500 applicativi**
- "Immaginate un'azienda dove una nave con **20.000 container** entra in un porto **ogni 15 minuti**, e non avete i computer"

Distribuzione combustibili (May 2021)

- 45% combustibili nella East Coast (aerei compresi)

- Distribuzione completamente sospesa ≈1 week
- Emergenza in 17 stati + Washington DC

Maastricht University (December 2019)

Ransomware attack: Maastricht University pays out $220,000 to cybercrooks

The Daily Swig
07 February 2020

- The university's networks were first breached on October 15 and 16, when two phishing emails were opened on two computers.
- The ransomware...then spread to **267 servers**

- The university became aware of the intrusion when computers flashed up ransom demands on **December 23**.

Enti Pubblici Italia 2021-2022 (Alcuni...)

- Regione Lazio
- Regione Sardegna
- Agenzia delle Entrate
- Ministero Transizione Ecologica
- Trenitalia
- Sogin (smantella centrali nucleari)
- SIAE
- Gestore Servizi Energetici
- ENI
- Comune di Palermo, Torino, **Gorizia**
- Università di Pisa
- ...

53 GB / 268.000 file

Parte 1-b:

Comprensione

Natura del software
Volontà e macchine
Attacchi mirati e non mirati

Dato di fatto:
"I computer sono differenti"

- **Ogni** sistema ha numerose **vulnerabilità** (caratteristiche indesiderate)
- Permettono uso **arbitrario** da parte di **chiunque**

- Non evidenti (ma ci sono)
- Chi le trova può sfruttarle

- **Unica** tecnologia della storia con questa caratteristica

Esempio: Microsoft (Aprile 2017)

- A ...vulnerability exists in the way that **Microsoft Office and WordPad** parse specially crafted files
- An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
- An attacker could exploit the vulnerability by sending a specially crafted file to the user and then convincing the user to open the file

Esempio: Google Chrome (Gennaio 2020)

Google Releases Security Updates for Chrome

Original release date: January 17, 2020

- Google has released **Chrome** version 79 for Windows, Mac, and Linux.
- This version addresses **vulnerabilities** that an attacker could exploit to **take control** of an affected system.

- ... a remote attacker ... to execute arbitrary code via a crafted HTML page.

Esempio: Whatsapp (Novembre 2019)

WhatsApp Remote Code Execution Triggered by Videos

threatpost

- ...could be exploited to launch remote code execution attacks on victims.
- Attackers can exploit the flaw merely by sending a target user a video — specifically, a specially crafted MP4 file

Lezione appresa

- UN click **può** essere sufficiente per **perdere il controllo** del proprio dispositivo / dati
  - Senza che ci sia una notifica evidente...
- L'inganno dell'utente è una tecnica potentissima e (in questi casi) necessaria
- Utente **crede** di eseguire una certa azione ed in realtà ne sta eseguendo una diversa

Vulnerability: Quante sono?

NATIONAL VULNERABILITY DATABASE

NIST National Institute of Standards and Technology

Search Results (Refine Search)

Search Parameters:

- Results Type: Overview
- Keyword (text search): chrome
- Search Type: Search Last 3 Months

There are **149** matching records.
Displaying matches **1** through **20**.

Search Results (Refine Search)

Search Parameters:

- Results Type: Overview
- Keyword (text search): acrobat reader
- Search Type: Search Last 3 Months

There are **28** matching records.
Displaying matches **1** through **20**.

"Tanto gli Apple non hanno i virus!"

NATIONAL VULNERABILITY DATABASE

NIST National Institute of Standards and Technology

Search Parameters:

- Results Type: Overview
- Keyword (text search): apple
- Search Type: Search Last 3 Years

There are **1,660** matching records.

Quali software?
Automobili (September 2016)

- From 12 miles away, while the car was moving
- ...remotely slam on the **brakes**, pop the **trunk** and fold in the **side mirror**...
- ...opened the **sunroof**, moved the power **seats**, and switched on the **turn signals**.

Quali software?
Pompe per diabetici (October 2016)

J&J warns diabetic patients: Insulin pump vulnerable to hacking

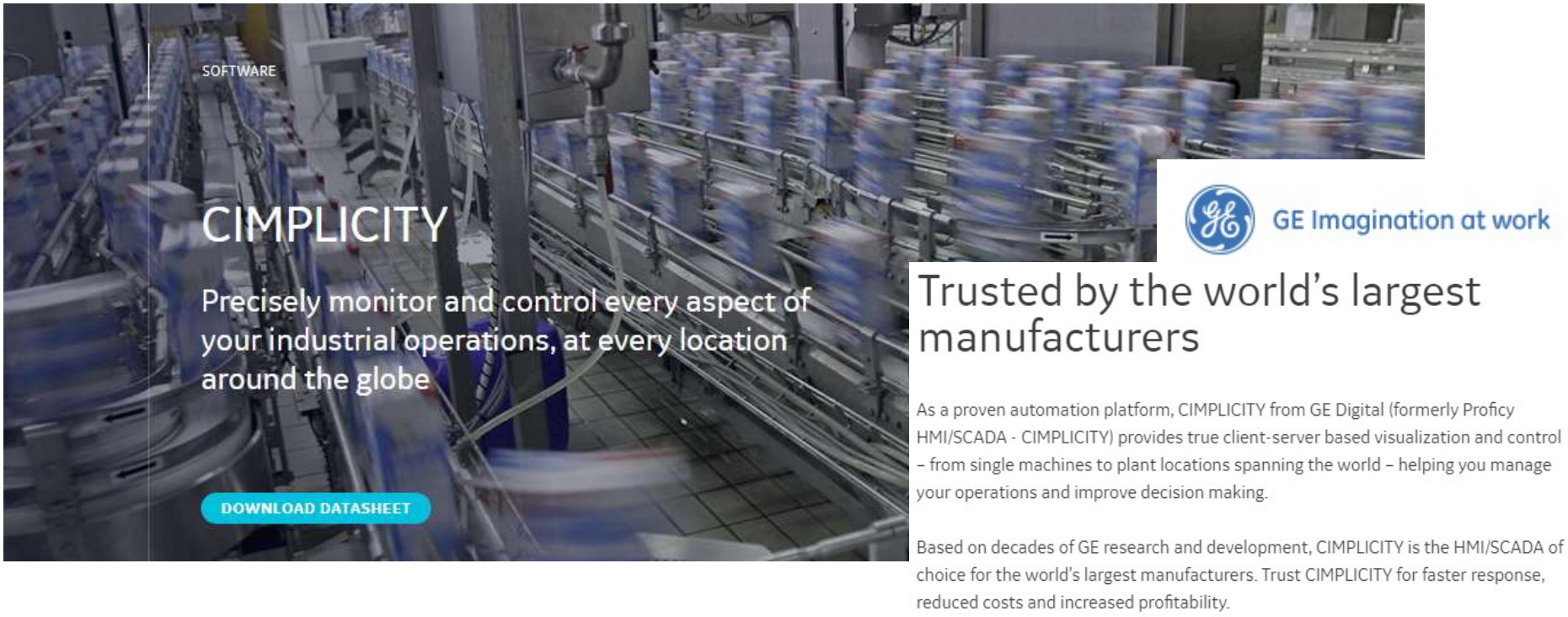
- ...a **remote attacker** can spoof the meter and **trigger unauthorized insulin injections**...
- ...these attacks could be performed from one to two kilometers away...

Quali software? Pacemakers (August 2017)

465,000 Patients Need Software Updates for Their Hackable Pacemakers, FDA Says MOTHERBOARD

- The recall has the goal of reducing the risk of hackers taking control of the pacemakers, potentially, harming the patients.

Quali software?
Industrial Control Systems



- Dighe, impianti chimici, acquedotti, energia, agricoltura, trasporti, energia elettrica...

Ahia...
(Ottobre 2017)

Advisory (ICSA-17-278-01A)

GE CIMPLICITY (Update A)

Original release date: October 05, 2017 | Last revised: October 10, 2017

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- Un **attaccante remoto** può eseguire **codice arbitrario**
- Non richiede capacità tecniche elevate

Avvisi
sicurezza informatica
dispositivi per
controllo industriale

- ICSA-17-087-01 : Siemens RUGGEDCOM ROX I
- ICSA-17-087-02 : 3S-Smart Software Solutions GmbH CODESYS Web Server
- ICSA-17-082-01 : LCDS - Leão Consultoria e Desenvolvimento de Sistemas LTDA
- ICSMA-17-082-01 : BD Kiestra PerformA and KLA Journal Service Applications Ha
- ICSA-17-047-01 : Rockwell Automation Connected Components Workbench
- ICSA-17-047-02 : Rockwell Automation FactoryTalk Activation
- ICSA-17-075-01 : LCDS - Leão Consultoria e Desenvolvimento de Sistemas LTDA
- ICSA-17-073-01 : Fatek Automation PLC Ethernet Module
- ICSA-17-068-01 : Schneider Electric ClearSCADA
- ICSA-17-066-01 : Schneider Electric Wonderware Intelligence
- ICSA-17-061-01 : Eaton xComfort Ethernet Communication Interface
- ICSA-17-061-02 : Schneider Electric Conext ComBox
- ICSA-17-061-03 : Siemens SINUMERIK Integrate and SINUMERIK Operate
- ICSA-17-059-01 : Siemens RUGGEDCOM NMS
- ICSA-17-054-02 : Red Lion Controls Sixnet-Managed Industrial Switches, Automat Ethernet Switches Vulnerability

Il mondo in cui viviamo (e vivremo)

- Trovare un settore che non dipende "pesantemente" dall'informatica

- **Impossibile**
  - Industry
  - Health
  - Transports
  - Energy (generation and distribution)
  - Finance
  - Public services
  - …

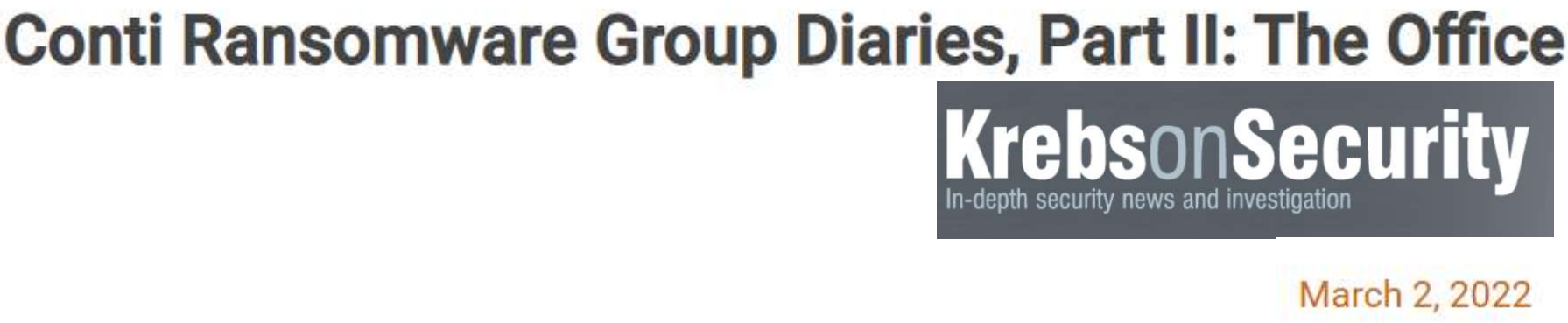
"Ho l'antivirus!"

- Rileva **poche** tipologie di attacco
- Quelle poche, inizia a rilevarle con **giorni** o **settimane** di ritardo

Wannacry (Maggio 2017): 30 minuti

150 paesi
100.000 organizzazioni

"Conti" Ransomware Group: Internal Chat



- Windows Defender aggiornato **ogni 4 ore**
- ≈100 "impiegati" in giro per il mondo modificano il loro malware **subito dopo** (**continuamente**)

Atteggiamento comune (SBAGLIATISSIMO)

- *"Vabbè, ma chi vuoi che venga ad attaccare **proprio me**?"*

Attack Focus (I)

- **Mirato**
  1. Scelgo il target
  2. Ispeziono il target vedo quali exploit posso usare

- Manuale ⇒ Costoso ⇒ **Poco** frequente

Attack Focus (II)

- **Non mirato**
  1. Tento di iniettare stesso exploit su molti target ("sparo nel mucchio")
  2. Vedo quali target ho colpito

- Automatizzabile
  ⇒ **Costi incrementali irrisori** (controintuitivo)
  ⇒ **Frequentissimo**

"Chi vuoi che attacchi proprio me?"

- Ragionamento **SBAGLIATISSIMO**
  - Gli attacchi più comuni sono **non mirati**
  - **Ognuno** è un potenziale bersaglio

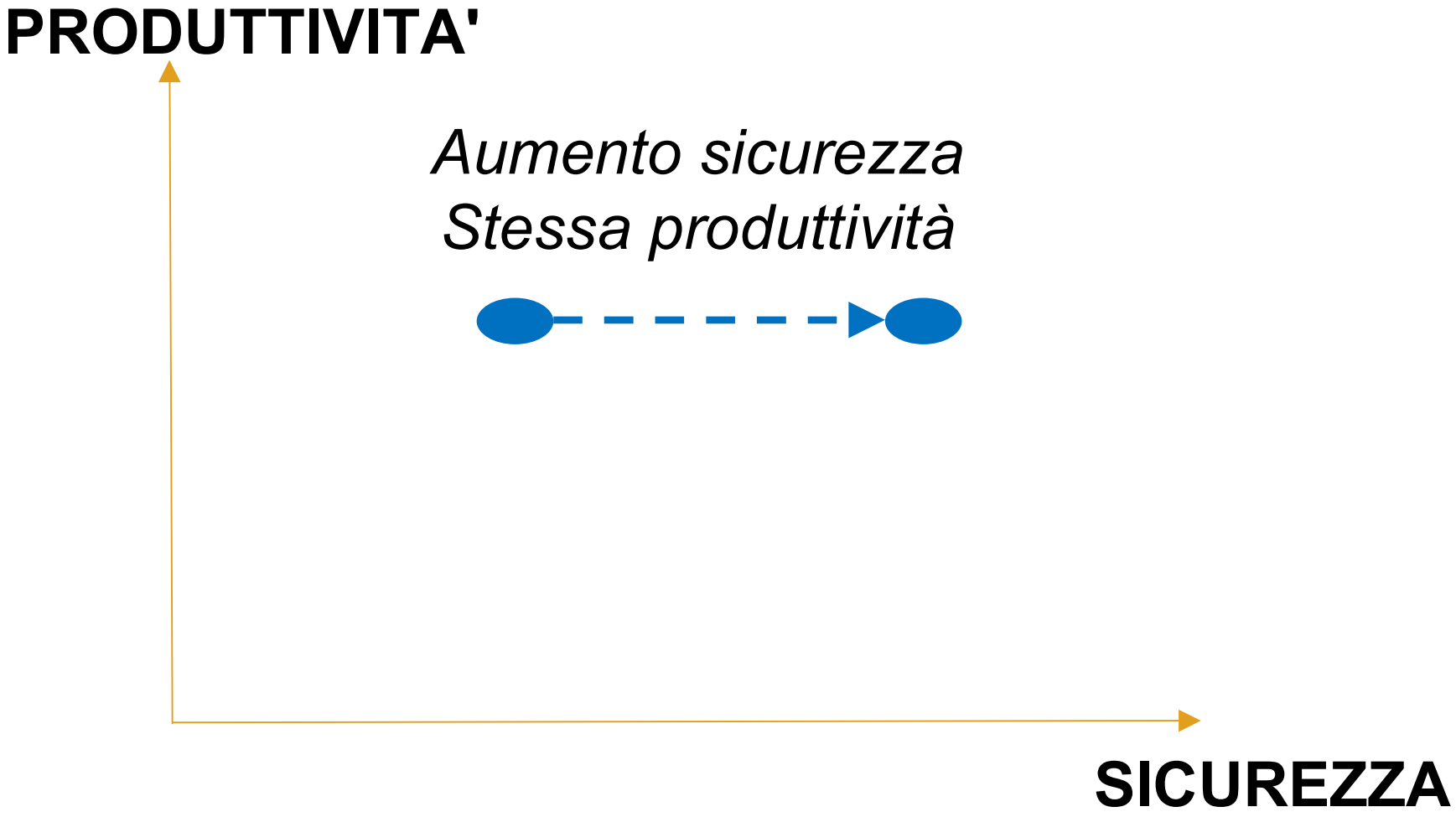
- Molto improbabile essere attaccato in quanto "Alberto Bartoli"
- Probabilissimo essere attaccato in quanto:
  - Uso email
  - Navigo su Web (Facebook, Paypal, Netflix, ...)
  - Windows 10 / Android 9
  - Adobe Acrobat versione 16.10.23
  - ...

"Investo X euro, faccio mettere a posto tutto"

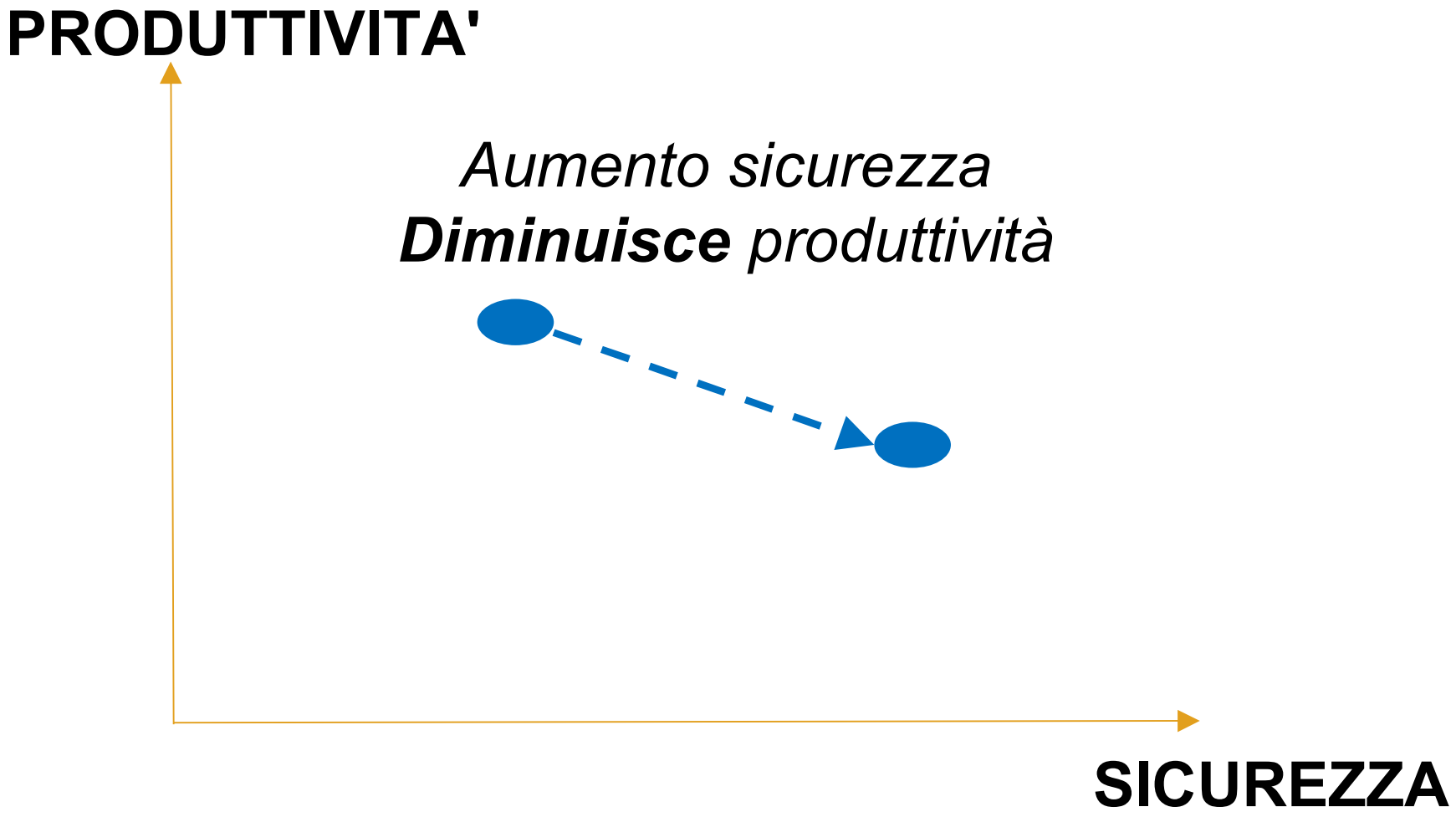
- Ragionamento **SBAGLIATISSIMO**
- **Non** è possibile una **soluzione puntuale** da demandare ai soli **tecnici**
  - Ognuno gestisce informazioni di potenziale **valore**
  - Ognuno è un **bersaglio**
  - Vulnerabilità e tecniche di attacco **cambiano**
  - Software diventano **obsoleti**

- Occorre un **processo continuo**
- Responsabilità di **tutti**

Produttività e Sicurezza: Sogno



Produttività e Sicurezza: Realtà



Security = Compromesso