Dipartimento
di Matematica
e Informatica

Corso di Laurea
in Informatica

Cervello e computer: bellezza e segreti dei bit di tutti i giorni

cybersecurity • intelligenza artificiale • realtà virtuale • Android

Ciclo di seminari di divulgazione informatica
in collaborazione con NOVA a.p.s.

NOVA

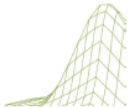
Ferrara, 8–12 Giugno 2020

Programma

Lunedì 8 Giugno: Carlo Giannelli
Cyber security: istruzioni per l'uso – Principi di sicurezza informatica

Martedì 9 Giugno: Guido Sciavicco
Come imparano le macchine – Principi di intelligenza artificiale

Mercoledì 10 Giugno: Marco Alberti
Neuroni di bit – Reti neurali e applicazioni



Giovedì 11 Giugno: Antonino Casile
Informatica e percezione sensoriale – L'ultima frontiera della realtà virtuale

Venerdì 12 Giugno: M. Roma, G. Turri, L. Travaglia – NOVA Ferrara
La nascita di un'app Android – Programmazione in Android

Disclaimer

- La presentazione, il filmato, i materiali e i contenuti in essi inclusi sono di proprietà dell'Università di Ferrara
- Il diritto morale d'autore ("Proprietà Intellettuale") appartiene ai singoli docenti/relatori dell'evento
- L'utilizzo è concesso per uso esclusivo e personale
- Nessun altro utilizzo può essere legittimamente esercitato senza la previa autorizzazione scritta dell'Ateneo e dei proprietari del diritto morale d'autore
- Qualunque abuso verrà perseguito a norma di legge
- Per ulteriori informazioni visitare il sito dmi.unife.it/stageInformatica

Università di Ferrara
Corso di Studi in Informatica

Cyber security: istruzioni per l'uso

Principi di sicurezza informatica

Prof. Carlo Giannelli
http://docente.unife.it/carlo.giannelli
08/06/2020

Dipartimento
di Matematica
e Informatica

Outline

- **Obiettivi della sicurezza**
- Tipiche minacce
- Mercato della sicurezza
- Alcuni attacchi
- Possibili contromisure

Obiettivi della sicurezza

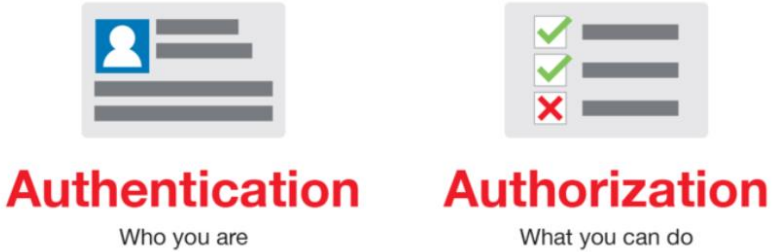
- La **protezione** delle
  - **risorse** da danneggiamenti volontari o involontari
  - **informazioni** mentre transitano sulla rete
- La **verifica delle identità** dell'interlocutore, in particolare la certezza che sia veramente chi dice di essere
- Il controllo dell'**autorizzazione** per l'accesso alle informazioni

Sicurezza: autenticazione e autorizzazione

- Autenticazione: **verifica dell'identità** dell'utente attraverso
  1. **Possesso di un oggetto**, ad esempio smart card
  2. **Conoscenza di un segreto**, solitamente password
  3. **Caratteristica personale fisiologica**, ad esempio impronta digitale, venature retina

- Autorizzazione: serve per specificare le **azioni concesse** a ogni utente

- Autenticazione ≠ Autorizzazione



Diversi aspetti relativi alla sicurezza informatica

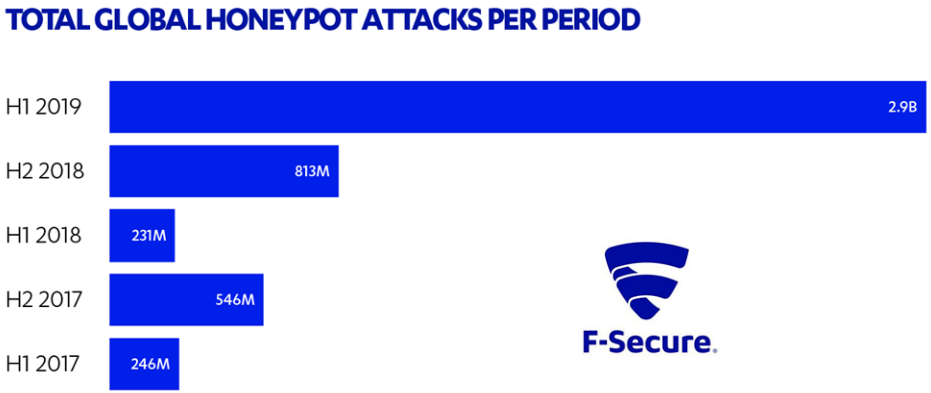
- **Riservatezza**: previene la lettura non autorizzata delle informazioni, ad esempio tramite messaggi cifrati; se intercettati, non rivelano comunque il contenuto
- **Integrità**: previene la modifica non autorizzata delle informazioni, ad esempio un messaggio spedito dal mittente è ricevuto tale e quale dal destinatario
- **Disponibilità**: garantire in qualunque momento la possibilità di usare le risorse, come servizi e applicazioni Web

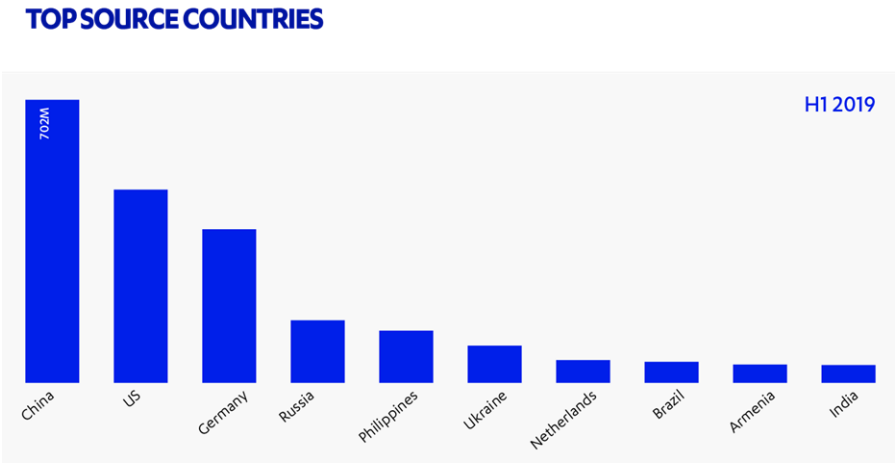
Outline

- Obiettivi della sicurezza
- **Tipiche minacce**
- Mercato della sicurezza
- Alcuni attacchi
- Possibili contromisure

Attacchi - Statistiche

- Le statistiche dimostrano che il numero degli attacchi nel 2019 è aumentato drasticamente!
- La maggior parte di questi provengono da Cina e Stati Uniti





Vettori d'attacco dei malware

Programma/codice utilizzato per **entrare nei sistemi** come server, computer, smartphone e altri dispositivi:

- **Virus:** programma malevolo in grado di replicarsi per diffondersi tra i file di un computer, ma anche da un computer a un altro
- **Worm:** simili a virus, ma si attivano autonomamente, ad esempio senza aprire file o link
- **Trojan Horse:** programma che nasconde il suo reale funzionamento all'interno di un altro software apparentemente utile e innocuo. L'utente, eseguendo o installando quest'ultimo programma, in effetti attiva anche il codice del trojan nascosto

Principali tipologie di malware

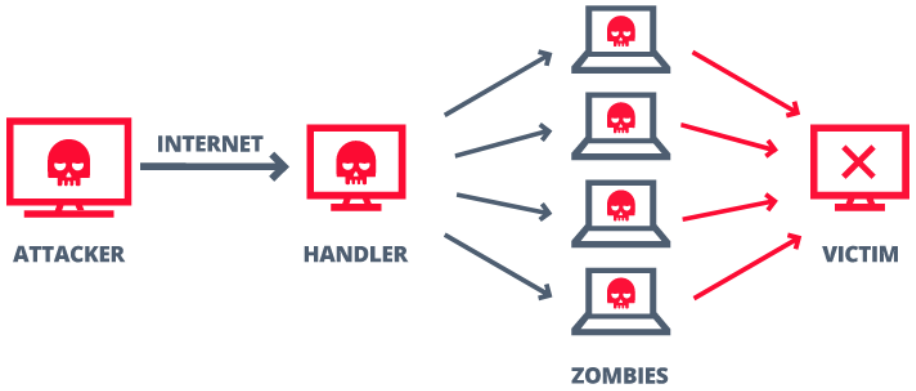
Programma/codice dannoso che **interferisce sul normale funzionamento** di un sistema:

- **Adware:** lancia messaggi pubblicitari sullo schermo, spesso all'interno di un browser Web
- **Spyware:** raccoglie informazioni sugli utenti e dati sulle abitudini di navigazione, l'utilizzo di Internet, ecc
- **Ransomware:** nega l'accesso ai file presenti in un computer richiedendo un compenso (tipicamente in Bitcoin) per poter averne nuovamente accesso
- **Denial of Service (DoS)**: ha lo scopo di rendere un server, un servizio o un'infrastruttura indisponibile attraverso l'invio di molte richieste dall'esterno

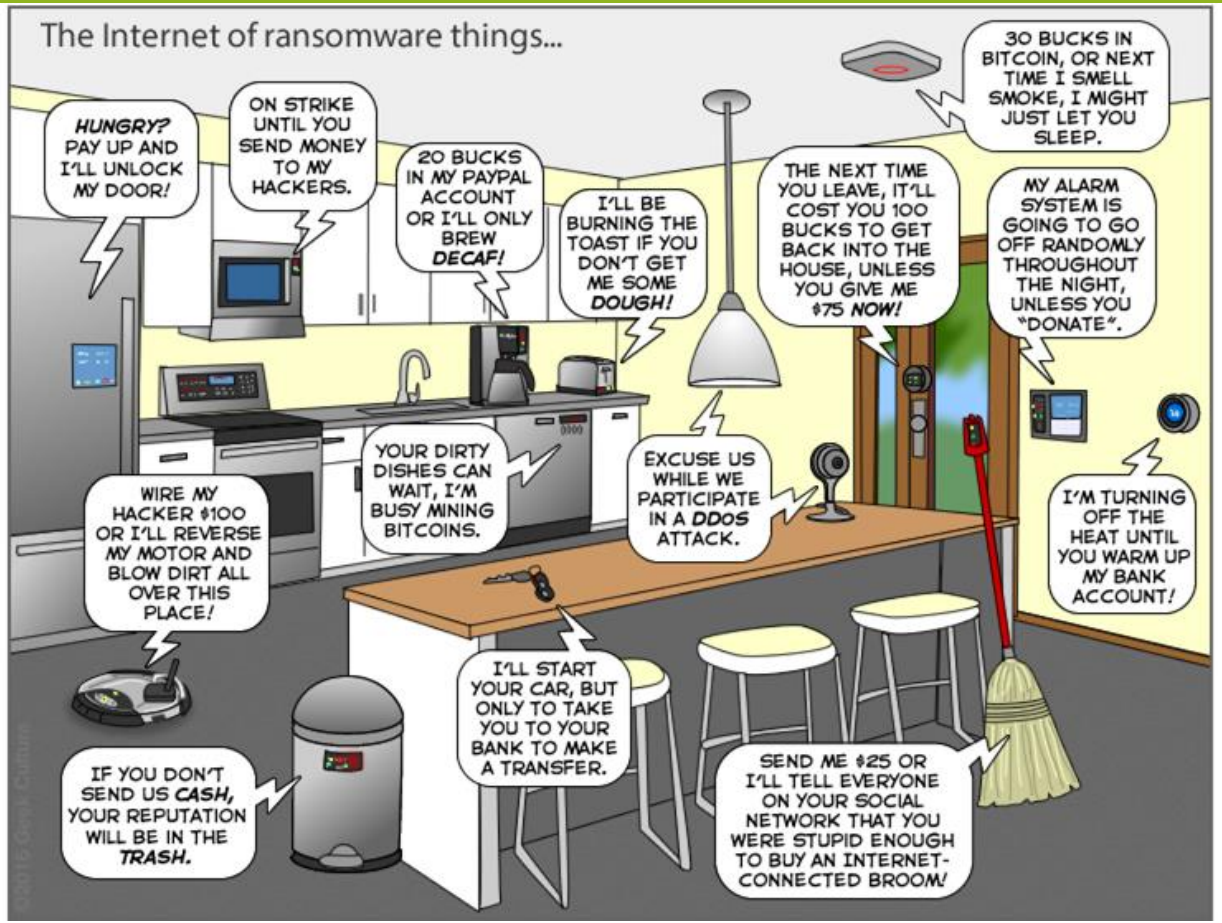
BotNet

- Rete controllata da un **bot-master** e composta da dispositivi detti **bot** o **zombie,** infettati da malware specializzati

- Il bot-master può controllare il sistema tramite accesso remoto
- I dispositivi connessi ad Internet al cui interno sussistono vulnerabilità possono diventare parte della BotNet
- I dispositivi infettati possono scagliare attacchi Distributed Denial of Service (DDoS) contro altri sistemi



The Internet of ransomware things…



Outline

- Obiettivi della sicurezza
- Tipiche minacce
- **Mercato della sicurezza**
- Alcuni attacchi
- Possibili contromisure

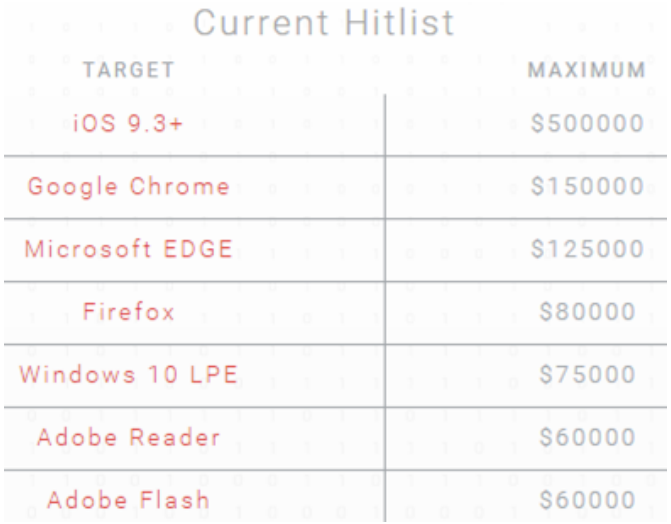
Ricerca di exploit come business

Exploit: sfrutta **un errore o una vulnerabilità** del software per provocare un certo comportamento inatteso, ad esempio per creare virus

Aziende specializzate nella **ricerca e vendita di exploit**:

- ReVuln, Vupen, Netragard, Exodus Intelligence
- Vendita di un bug: $35-160K

Stato-nazione come acquirenti: “Israel, Britain, Russia, India and Brazil are some of the biggest spenders. North Korea is in the market, as are some Middle Eastern intelligence services. Countries in the Asian Pacific, including Malaysia and Singapore, are buying, too” --- **NY Times** (July 2013)



Ricompensa Exodus zero-day

Mercato delle vulnerabilità: legale

Opzione 1: bug bounty programs (2019)

- Google: min. $300 per bug, max senza limite
- Facebook: min. $500 per bug, max senza limite
- Microsoft: min. $15K per bug, max $250K

Opzione 2: vulnerability brokers

- Zero Day Initiative: $145K
- Pwn2Own competition: $545K (totale di tutte le categorie)

Mercato delle vulnerabilità: illegale

Opzione 3: mercato nero e “grigio”

- Fino a $100-250K (difficile da verificare)
- Vulnerabilità zero-day per iOS venduta per $500K (presumibilmente)

[remote exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
22-01-2018	Yandex Mail reset password (bypass 2FA) 0day Exploit	tricks	66		R	D	-	√	B 5.714	0day Today Team
10-01-2018	WhatsApp Remote Code Execute (poison autoclick link) 0day Exploit	Android	101		R	D	-	√	B 5.429	0day Today Team
06-01-2018	Adobe Acrobat Reader Remote Code Execute 0day Exploit	windows	82		R	D	-	√	B 6.429	0day Today Team
20-12-2017	Android 8.x.x Remote Execute 0day Exploit	Android	42		R	D	-	√	B 17.286	0day Today Team
02-12-2017	Microsoft Office Word 2013 Universal 0day Exploit (python builder)	windows	298		R	D	-	√	B 5	0day Today Team
25-10-2017	Microsoft Office Word 2003/2007/2010 Remote code execute and Privilege Escalation 0day	windows	307		R	D	-	√	B 5.714	0day Today Team
18-12-2016	Twitter accounts lock / restore and change @twitter name 0day Exploit	tricks	138		R	D	-	√	B 5.714	Spain Squad
05-12-2016	Windows 8.X Remote Code Execution and Privilege Escalation Exploit	windows	81		R	D	-	√	B 10	0day Today Team

[local exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
06-10-2017	Windows server 2008 R2 Local Privilege Escalation 0day	windows	348		R	D	-	√	B 12.286	0day Today Team

[web applications]

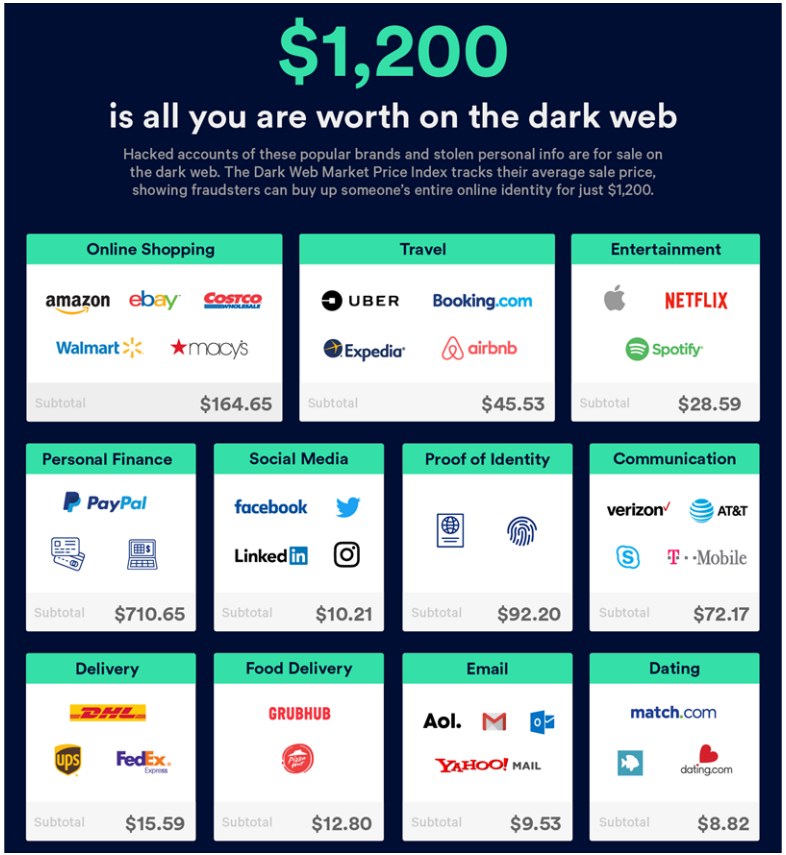
-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
26-02-2018	Joomla 3.8.5 SQL Injection / Shell upload Vulnerabilities	php	40		R	D	-	√	B 5.571	0day Today Team
14-02-2018	Magento 2.2 Remote Code Execution 0day Exploit	php	49		R	D	-	√	B 5.286	0day Today Team
05-02-2018	Invision Power Board 4.2.7 Shell Upload / Privilege Escalation 0day Exploit	php	31		R	D	-	√	B 5	0day Today Team
31-01-2018	WordPress 4.9.2 - SQL Injection Vulnerability	php	48		R	D	-	√	B 5.429	0day Today Team
27-01-2018	Joomla 3.8.3 Remote Code Execution and Privilege Escalation Exploit (0day)	php	73		R	D	-	√	B 6.143	0day Today Team

Mercato dei malware: illegale

- **Pay-per-installazione** su macchine compromesse
  - Stati Uniti: download da $100-150 / 1000
  - Può essere utilizzato per inviare spam, organizzare attacchi Denial of Service, eseguire frodi, ospitare siti Web truffa
- **BotNet in affitto**
  - DDoS: da $20/ora
  - Spam: da $10/1.000.000 di email
- **Strumenti e servizi**
  - Trojan di base ($3-10), rootkit di Windows ($300), e-mail, SMS, strumenti di spamming ICQ ($30-50), configurazione e supporto BotNet ($200/mese, ecc.)

Mercato dei dati: illegale

- Conti Paypal: in media $247
- Airbnb: meno di $8
- Identità digitale completa "fullz": ~ $1,200



Outline

- Obiettivi della sicurezza
- Tipiche minacce
- Mercato della sicurezza
- **Alcuni attacchi**
- Possibili contromisure

Siamo sicuri che tutto sia realmente protetto?

Pensare come un attaccante!

Spesso il punto debole è più banale di quanto si possa immaginare…

Password deboli - Top 10 password più utilizzate

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]	2019[13]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1111111
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	abc123
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	1234567
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty	password1
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou	12345

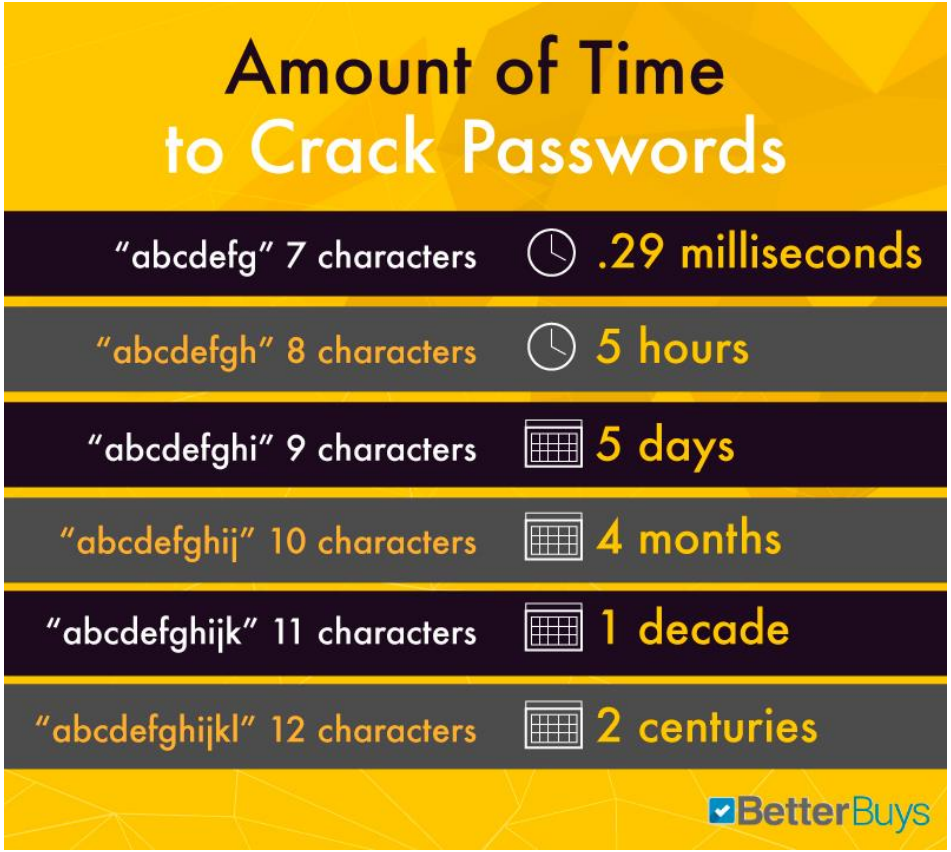
Come scoprire una password?

Cracker per indovinare password:

- **Attacco basato su dizionario:** il più comune, consiste nello scorrere ciclicamente un dizionario di password noto, provando ogni password presente nel dizionario per ciascun account noto
- **Forza bruta:** più aggressivo, si concentra principalmente su password brevi. Un cracker di password a forza bruta prende di mira un certo numero di caratteri e quindi testa ogni combinazione di caratteri della lunghezza massima o meno. Questo può essere un lungo processo.

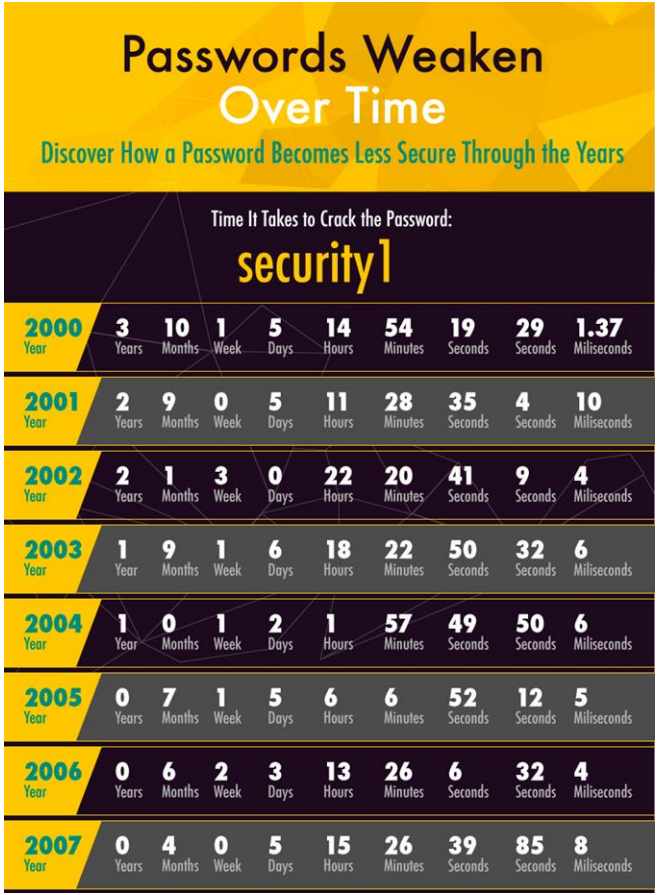
Lunghezza di una password

Quanto vale la **lunghezza** di una password **in tempo** per un attacco a forze bruta?



Efficacia di una password nel tempo

Perché è necessario **cambiare spesso** la password che utilizziamo?



Passwords Weaken Over Time

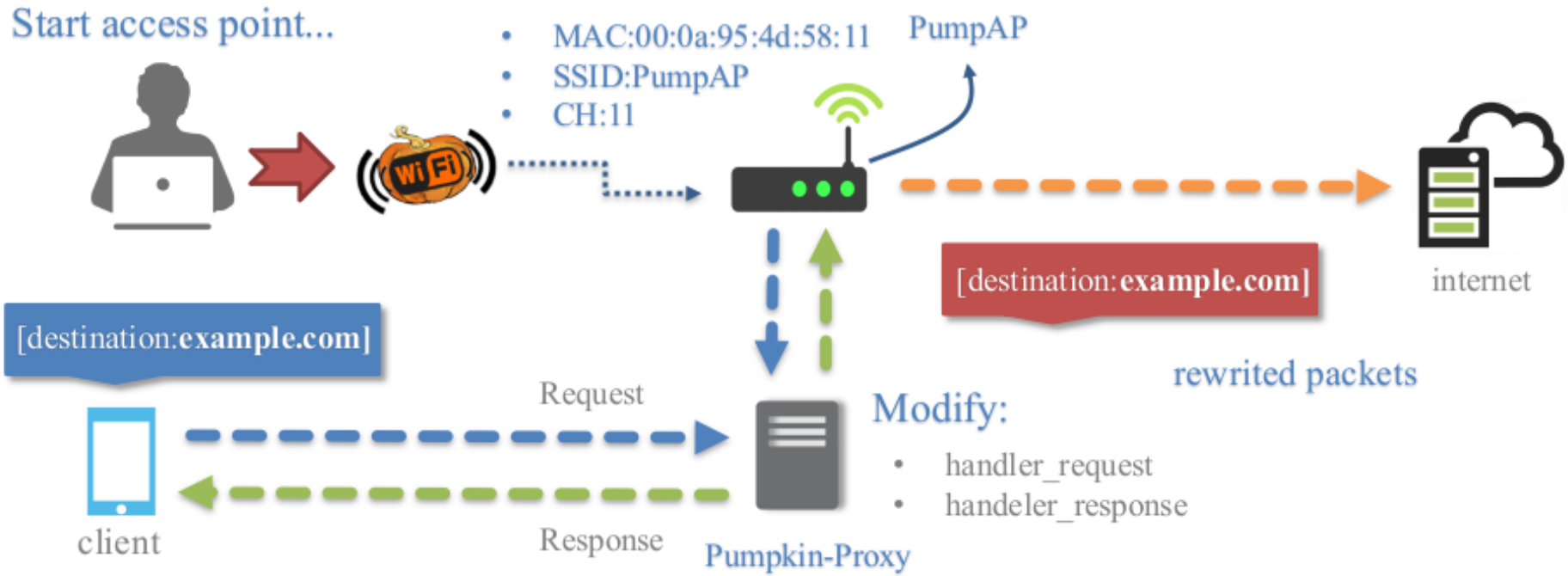
Discover How a Password Becomes Less Secure Through the Years

Time It Takes to Crack the Password: **security1**

2000 Year	3 Years	10 Months	1 Week	5 Days	14 Hours	54 Minutes	19 Seconds	29 Seconds	1.37 Miliseconds
2001 Year	2 Years	9 Months	0 Week	5 Days	11 Hours	28 Minutes	35 Seconds	4 Seconds	10 Miliseconds
2002 Year	2 Years	1 Months	3 Week	0 Days	22 Hours	20 Minutes	41 Seconds	9 Seconds	4 Miliseconds
2003 Year	1 Year	9 Months	1 Week	6 Days	18 Hours	22 Minutes	50 Seconds	32 Seconds	6 Miliseconds
2004 Year	1 Year	0 Months	1 Week	2 Days	1 Hours	57 Minutes	49 Seconds	50 Seconds	6 Miliseconds
2005 Year	0 Years	7 Months	1 Week	5 Days	6 Hours	6 Minutes	52 Seconds	12 Seconds	5 Miliseconds
2006 Year	0 Years	6 Months	2 Week	3 Days	13 Hours	26 Minutes	6 Seconds	32 Seconds	4 Miliseconds
2007 Year	0 Years	4 Months	0 Week	5 Days	15 Hours	26 Minutes	39 Seconds	85 Seconds	8 Miliseconds
2008 Year	0 Years	4 Months	3 Week	4 Days	1 Hours	26 Minutes	2 Seconds	13 Seconds	5 Miliseconds
2009 Year	0 Years	4 Months	3 Week	2 Days	8 Hours	9 Minutes	8 Seconds	56 Seconds	5 Miliseconds
2010 Year	0 Years	4 Months	1 Week	4 Days	19 Hours	7 Minutes	57 Seconds	74 Seconds	6 Miliseconds
2011 Year	0 Years	4 Months	1 Week	2 Days	12 Hours	25 Minutes	23 Seconds	33 Seconds	6 Miliseconds
2012 Year	0 Years	4 Months	0 Week	0 Days	21 Hours	11 Minutes	42 Seconds	77 Seconds	0.9 Miliseconds
2013 Year	0 Years	3 Months	3 Week	5 Days	23 Hours	36 Minutes	29 Seconds	81 Seconds	10 Miliseconds
2014 Year	0 Years	3 Months	3 Week	1 Days	0 Hours	39 Minutes	45 Seconds	23 Seconds	9 Miliseconds
2015 Year	0 Years	3 Months	1 Week	6 Days	14 Hours	44 Minutes	19 Seconds	66 Seconds	5 Miliseconds
2016 Year	0 Years	2 Months	4 Week	1 Days	10 Hours	12 Minutes	11 Seconds	31 Seconds	3 Miliseconds

Più tempo passa meno è efficace!

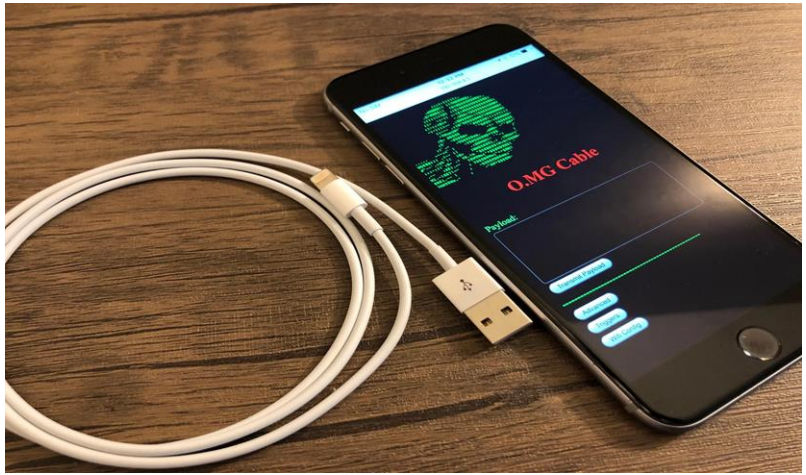
Accesso a reti pubbliche?

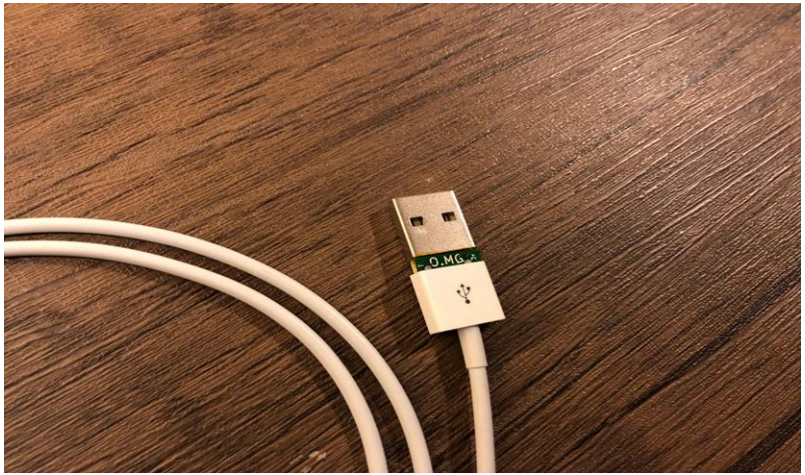


Rubber Ducky

- Una volta collegata ad un computer **viene riconosciuta come una tastiera** e non come una memoria
- Al suo interno è possibile salvare degli **script da eseguire non appena la chiavetta viene inserita**: automatizzare le azioni possibili tramite una tastiera, quindi aprire applicazioni, digitare comandi, reverse-shell, ecc..
- Linguaggio di scripting di Rubber Ducky decisamente semplice: comandi come “GUI r” ad esempio per aprire una finestra “Esegui” di Windows
- Vincoli:
  - dobbiamo avere accesso fisico alla macchina
  - la macchina vittima dev’essere sbloccata

Un semplice cavo USB…

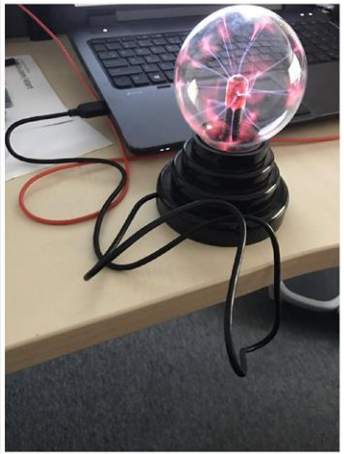


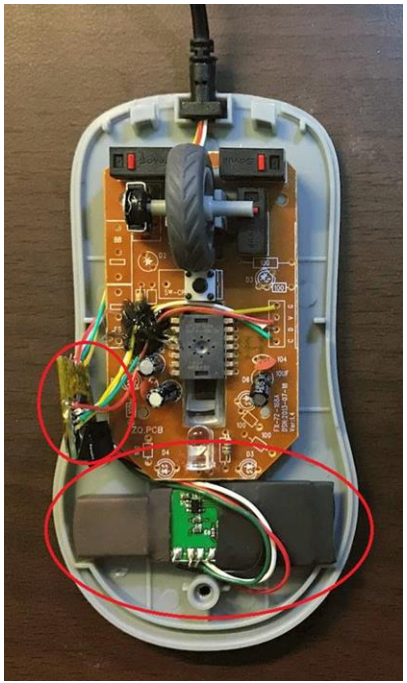


- Non appena il cavo è collegato, può essere controllato tramite l'interfaccia di rete wireless che risiede all'interno del cavo
- Il cavo consente di creare, salvare e trasmettere nuovi payload da remoto

WiFi HID Injector

- Sfera al plasma con cavo USB
- In realtà è anche un emulatore di tastiera e mouse, gestito da remoto via Wi-Fi





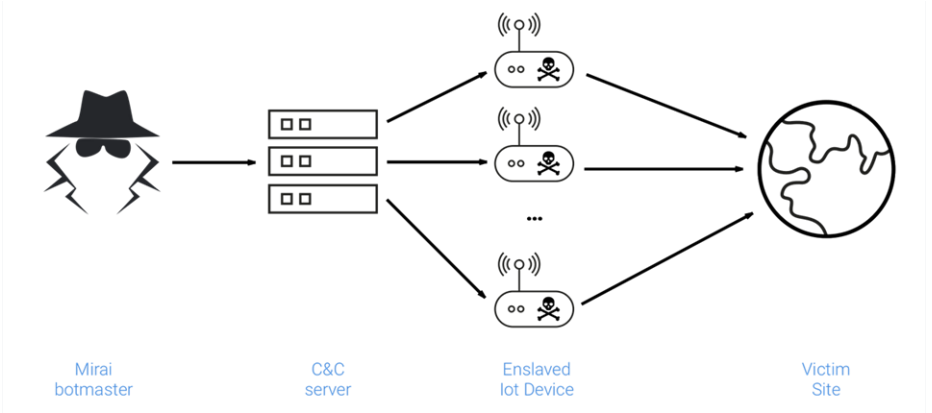
Bancomat via USB

- Attacco ai bancomat tramite vulnerabilità del software:
  - possibilità di sfruttare alcune vulnerabilità nel software di interazione con l'utente
  - per quanto si sa, non è mai stata utilizzata in un vero attacco

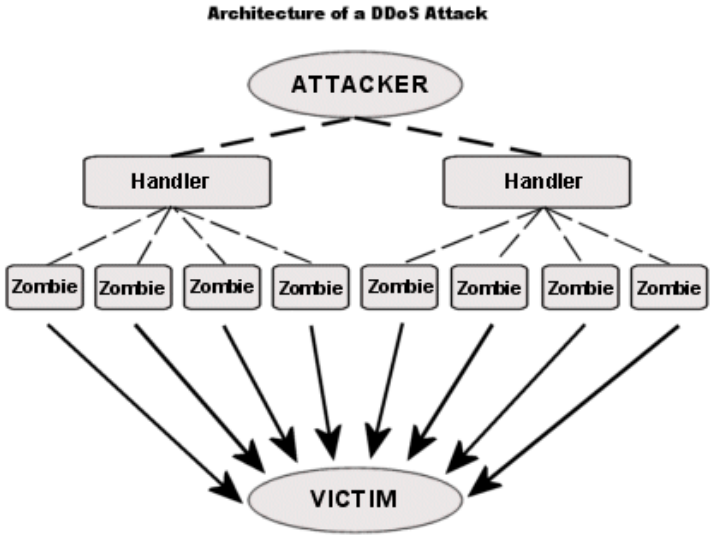
- Accesso allo sportello automatico tramite una rete interna precedentemente compromessa
- **Accesso fisico al bancomat via USB**

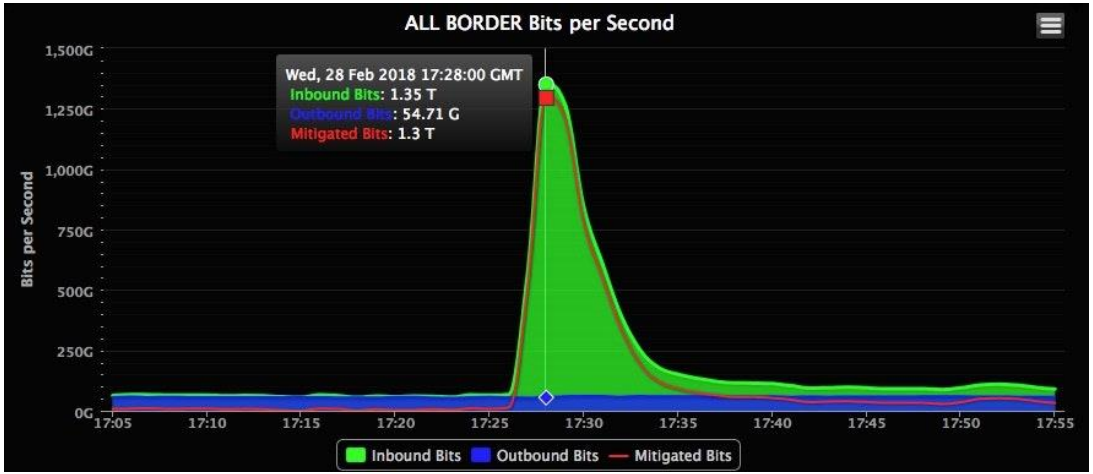
Malware Mirai

- Malware progettato per operare su **piccoli dispositivi connessi a Internet**, specialmente dispositivi IoT: home router, monitor qualità dell'aria, telecamere di sorveglianza
- **Dispositivi parte di una BotNet** (ancora oggi attiva) che può essere usata per attacchi informatici su larga scala
- **Infettati fino a 600000 dispositivi**, al momento è solo la 4° BotNet a livello mondiale



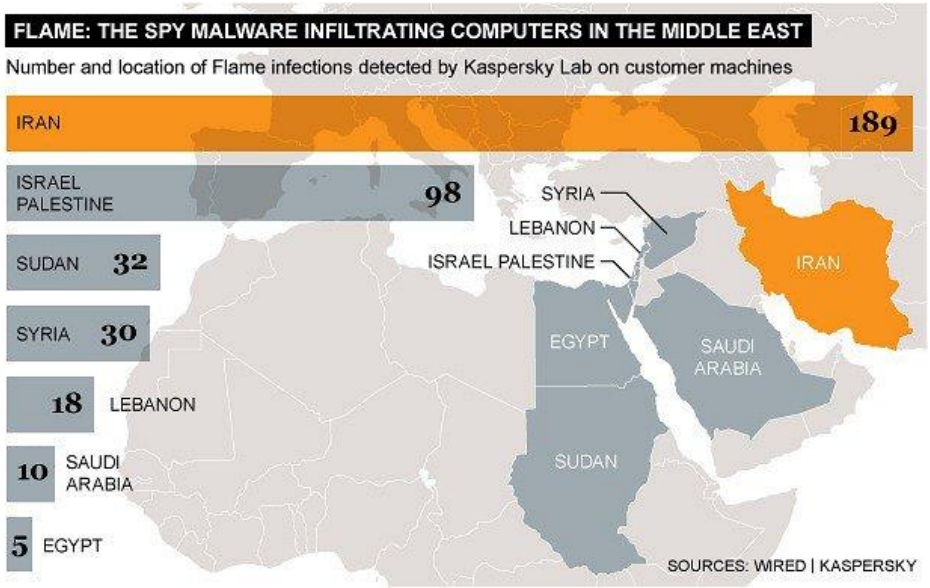
28/02/2018: attacco DDoS a GitHub





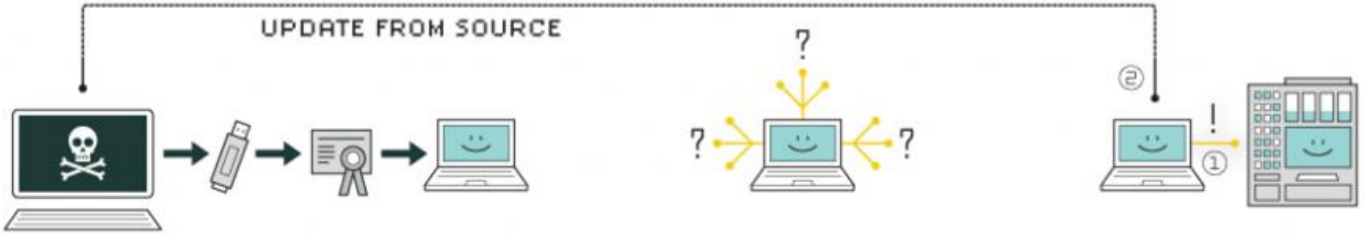
Malware Stuxnet

- Creato nel 2006 da una (probabile) collaborazione fra gli Stati Uniti e lo stato di Israele
- **Virus** informatico con lo scopo di **sabotare centrali nucleari**
- Il virus doveva danneggiare le centrifughe delle centrali iraniane, impedendo la rilevazione dei malfunzionamenti e della presenza del virus stesso



Zero Days (2016): http://www.zerodaysfilm.com/

Malware Stuxnet: funzionamento



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

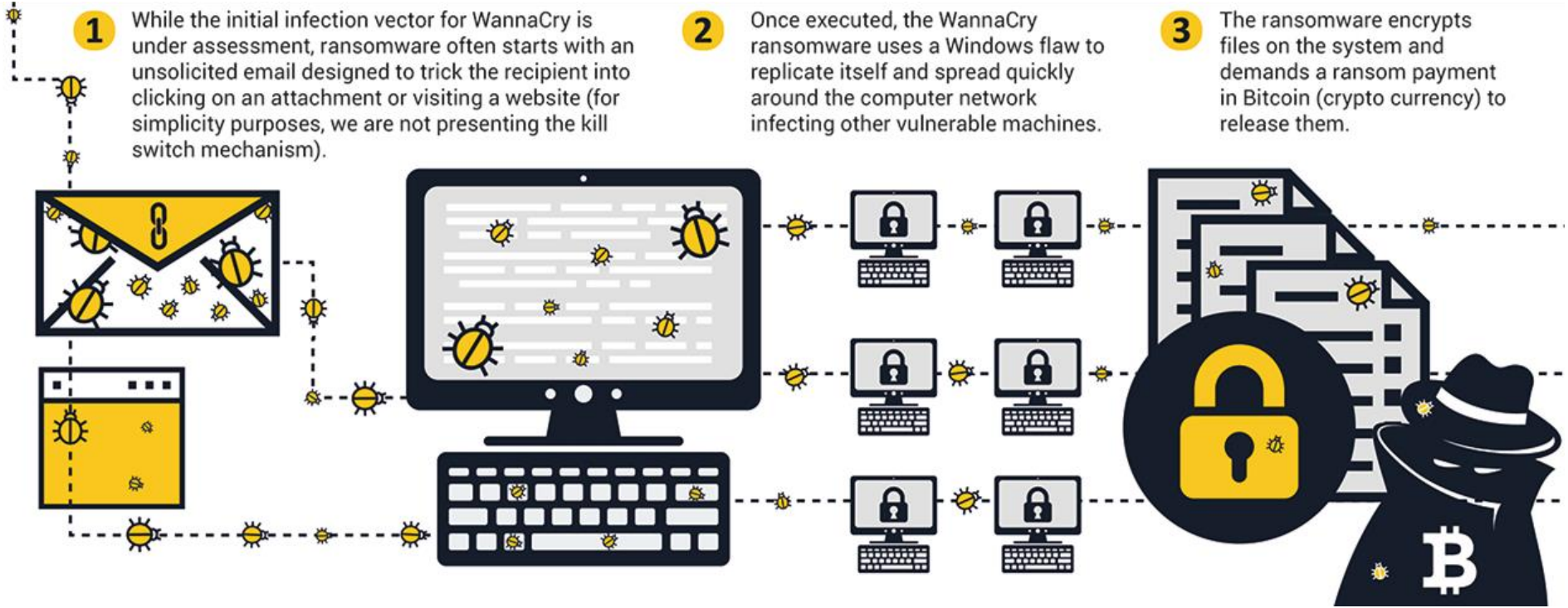
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Malware WannaCry



Industria 4.0: l'informatica dentro la fabbrica

- Attacco Ransomware a Bonfiglioli nel Giugno 2019, riscatto da 2.5M€
  - https://www.ansa.it/emiliaromagna/notizie/2019/07/02/cyber-attacco-ad-azienda-bolognese_69ca42c7-460a-4989-8e0d-d0d573473980.html
- Accesso tramite infrastruttura IT, per poi bloccare anche l'attività di produttiva!
- Durata aggressione 3 giorni, 10 giorni per ripulire tutto

- Forse intrusione iniziale effettuata con **malware 0 day**
  - identificazione basata su minacce note inefficace
  - fondamentale uso di anomaly detection (dettagli nel seguito)

- Rete globale composta da **molteplici sottoreti** con diversi amministratori
  - non sempre noto l'insieme complessivo di nodi e servizi attivi
  - nodi "deboli" come entry point, poi escalation orizzontale

Quali insegnamenti?

- **Monitoraggio 24h della rete**
  - **conoscere se stessi**, con elenco aggiornato e preciso di nodi presenti, servizi attivi, accesso utenti, traffico in ingresso/uscita
  - OK antivirus, ma **anomaly detection** per distinguere tra comportamento / traffico lecito e anomalo, sia dal punto di vista quantitativo che qualitativo

- **Backup** e che sia mantenuto in un **dominio distinto**
  - backup nello stesso dominio OK per fault tolerance, non sufficiente per cyberattacchi

→ Molte (molte) altre aziende (anche della zona) vittime di recenti cyberattacchi (non resi pubblici) con **blocco della produzione per giorni/settimane**!

Outline

- Obiettivi della sicurezza
- Tipiche minacce
- Mercato della sicurezza
- Alcuni attacchi
- **Possibili contromisure**

Ciclo di vita di un attacco 1/2

1. **Gathering delle informazioni:** analisi della portata dell'attacco valutando le difese disponibili di un sistema e le sue potenziali vulnerabilità:
   a. *logiche*: vulnerabilità del software (es. zero day)
   b. *fisiche*: accesso diretto a un endpoint (es. sensore)
   c. *umane*: ad esempio dipendente insoddisfatto (social engineering)
2. **Compromissione iniziale:** accesso a una rete di sistema e/o piattaforma sfruttando una delle vulnerabilità identificate
3. **Comando e controllo:** una volta all'interno della piattaforma, installazione di un software dannoso (ad esempio strumenti di accesso remoto) per riaccedere rapidamente al sistema

Ciclo di vita di un attacco 2/2

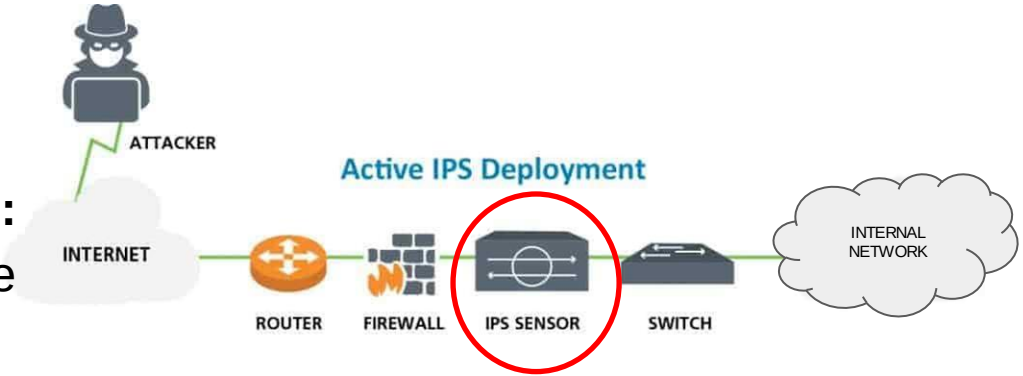
4. **Escalation dei privilegi:** incrementare i propri privilegi una volta all'interno del sistema, ad esempio ottenendo certificati validati da una Public Key Infrastructure (PKI) o con l'installazione di key logger per ottenere password
5. **Spostamento laterale:** scansione della rete interna al fine di trovare obiettivi aggiuntivi, ad esempio per accedere ad altri dispositivi ed eseguire scansioni di vulnerabilità interne
6. **Raggiungimento del target:** ha accesso alle risorse obiettivo, ad esempio per ottenere o cancellare file o informazioni in database o anche solo per modificare le configurazioni o disattivare dei dispositivi

4 fasi della sicurezza

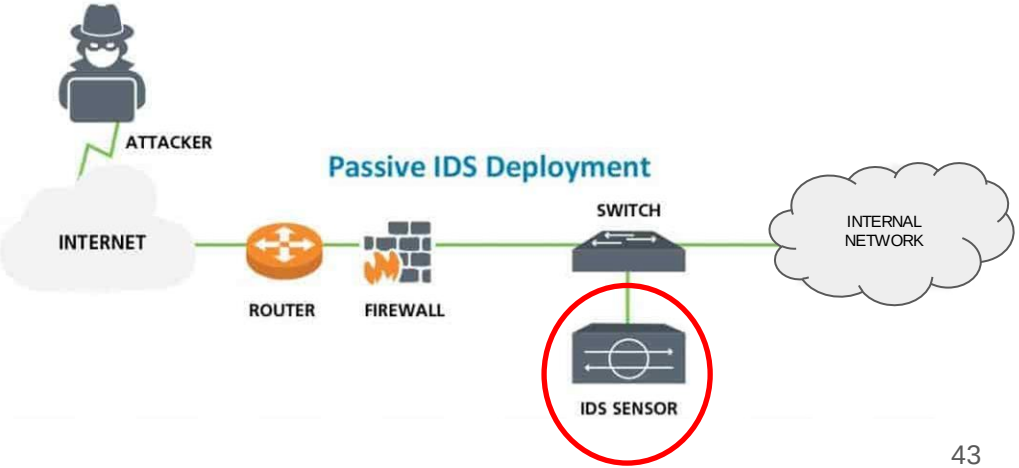
1. **Prevention**: implementare misure per prevenire lo sfruttamento delle vulnerabilità del sistema
2. **Detection**: rilevare prontamente il problema permette di intraprendere delle azioni prima che questo si diffonda
3. **Automation**: quando possibile, cercare di automatizzare le azioni di risposta alle operazioni di prevention e detection
4. **Response**: sviluppare un piano appropriato di intervento in caso di violazione con individuazione delle responsabilità e delle azioni da intraprendere

Prevenzione e rilevamento

- **Intrusion Prevention System (IPS):** impedire a un attaccante di accedere a risorse critiche preventivamente



- **Intrusion Detection System (IDS):** controllare continuamente le risorse critiche al fine di rilevare attacchi



Differenze fra IDS e IPS

Esistono diverse differenze tra questi due tipi di sistemi:

- **Margine di azione:** IDS emette avvisi solo per potenziali attacchi, mentre IPS agisce attivamente contro di essi
- **Controllo del traffico:** non tutto il traffico può passare attraverso un IDS ma deve invece passare attraverso un IPS
- **Suscettibilità a falsi positivi:** in caso di falsi positivi un IDS può solo emettere avvisi, mentre un IPS può eseguire importanti azioni (ma che potrebbero causare perdita dati o isolamento di un sistema)

Tecniche di rilevamento

Due principali approcci di rilevamento delle intrusioni per rilevare le minacce presenti sulla rete o su un host:

- Rilevamento basato su **signature:** uso di un database con tutte le firme (signature) di attacchi/minacce note
- Rilevamento basato su **anomalia:** incentrato sulla comparazione di attività classificate come “normali” e altre classificate come anomale

Rilevamento basato su signature

- **Signature**: tipico footprint o modello associato a un attacco in corso a livello di rete o di host. Ad esempio, una sequenza di byte (in un file o in un payload) o un processo (software non autorizzato o accesso alla rete non autorizzato)
- Si basa su un **elenco preprogrammato di comportamenti di attacco noti** che attivano una notifica di avviso
- La stessa tecnica che utilizzano i classici antivirus

Rilevamento basato su anomalia

- **Monitorare che il traffico e/o un host rispetti un modello di comportamento** classificato come “normale”**,** emettendo un **allarme** ogni volta che si rileva una qualsiasi **deviazione da tale modello** di comportamento
- Approccio complesso che necessita di una **fase di addestramento** durante la quale "apprendere" il comportamento normale (tecniche di apprendimento automatico)

In conclusione...

- Cybersecurity come **processo complesso e articolato**, che coinvolge aspetti molto eterogenei:
  - **hardware**: come renderlo sicuro anche se non lo gestiamo direttamente?
  - **software**: come produrlo sicuro? come aggiornarlo in modo sicuro?
  - **persone**: l'elemento umano spesso come tallone d'Achille!
- **Continua evoluzione**: cattivi con nuovi obiettivi e strumenti di attacco, buoni con sfide sempre diverse
- **Contesto ampio**: ambito internazionale, con nuove sfide attuali legate al mondo dell'industria che sempre più utilizza l'informatica → Industria 4.0!

“La sicurezza è un processo, non un prodotto”

Bruce Schneier

(esperto internazionale di sicurezza)

Competence Center Bi-REX per l'Industria 4.0

- Università di Ferrara attivamente coinvolta in un progetto di cyber security e Industria 4.0 del competence center Bi-Rex https://bi-rex.it/ con partner industriali quali SACMI, IMA e Siemens

Grazie per l'attenzione!

Domande? Curiosità?

Dipartimento di Matematica e Informatica