Attacco e difesa

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

Attacco e difesa

- Chi sono i cattivi
- Tipi di attacco
- Gestione degli incidenti (Damage Control)
- Digital Forensic
- Comportamenti dell'attacante (criminologia)
- Come fanno i cattivi ad incassare? Due parole su Bitcoin (e Blockchain)

....

Chi sono i “cattivi” ?

Conosciamo tutti i nostri vicini? Pensiamo a Internet come a un immenso vicinato virtuale dove è impossibile conoscere tutti ed è difficile distinguere i buoni dai cattivi.

I criminali esistono ma hanno un raggio di azione limitato; i cybercriminali sono invece dappertutto e sono anche nostri vicini di rete.

Sicuramente l’adozione di una suite di prodotti per la sicurezza dei computer e delle reti (aziendali e casalinghe) è necessaria, ma soprattutto occorre conoscere con chi e cosa si ha a che fare tutti i giorni. Solo conoscendo quali sono i nemici online si evita di divenire vittime.

In questa prima parte parleremo dei cattivi “di professione”, in seguito vedremo i cattivi “occasionali” o “inconsapevoli”.

Chi sono i “cattivi” ?

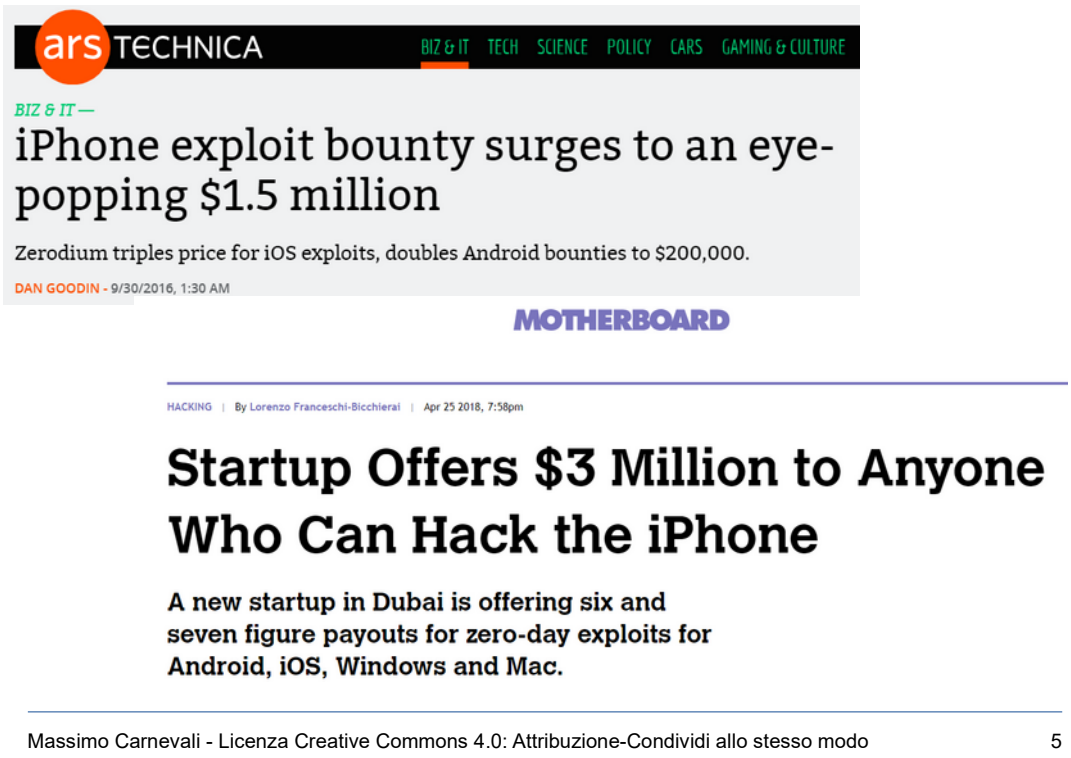
Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	$5,000–$30,000
Mac OS X	$20,000–$50,000
Android	$30,000–$60,000
Flash or Java Browser Plug-ins	$40,000–$100,000
Microsoft Word	$50,000–$100,000
Windows	$60,000–$120,000
Firefox or Safari	$60,000–$150,000
Chrome or Internet Explorer	$80,000–$200,000
IOS	$100,000–$250,000

Essenzialmente gente che lo fa per soldi ovviamente.

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Chi sono i “cattivi” ?



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BIZ & IT —

iPhone exploit bounty surges to an eye-popping $1.5 million

Zerodium triples price for iOS exploits, doubles Android bounties to $200,000.

DAN GOODIN - 9/30/2016, 1:30 AM

MOTHERBOARD

HACKING | By Lorenzo Franceschi-Bicchierai | Apr 25 2018, 7:58pm

Startup Offers $3 Million to Anyone Who Can Hack the iPhone

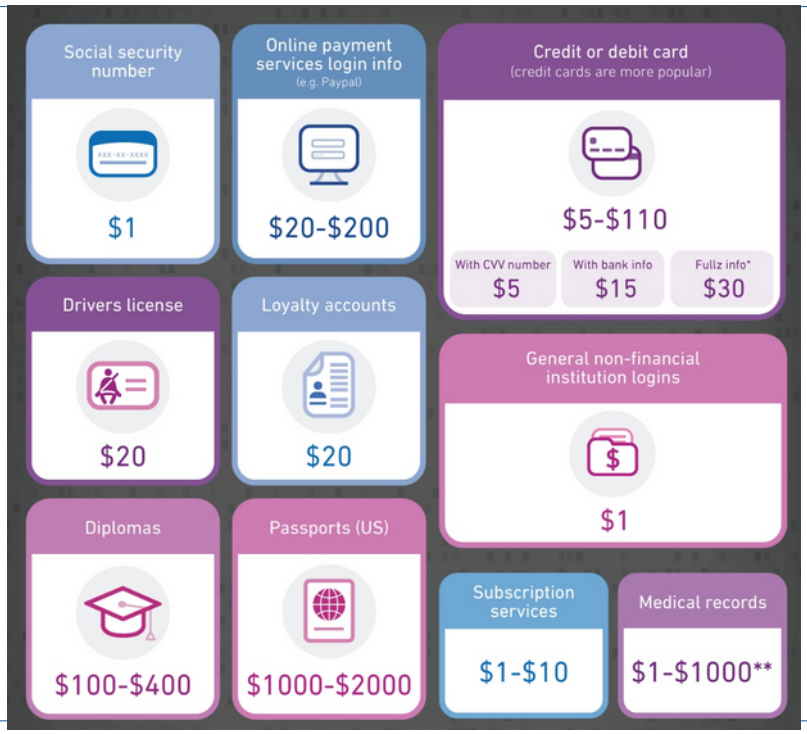
A new startup in Dubai is offering six and seven figure payouts for zero-day exploits for Android, iOS, Windows and Mac.

 5

Essenzialmente gente che lo fa per soldi ovviamente.

Si possono fare soldi anche legalmente con gli “Zero Day”: Bug Bounty programs.

Chi sono i “cattivi” ?



https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

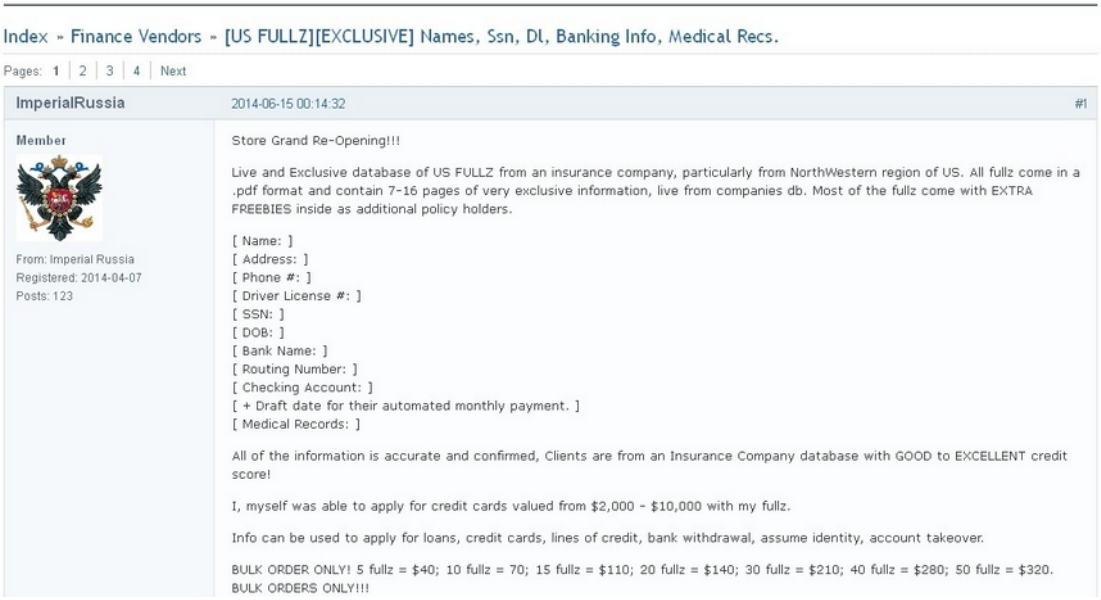
……..

Chi sono i “cattivi” ?

Figure 8. Botnet services.

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Chi sono i “cattivi” ?



Index » Finance Vendors » [US FULLZ][EXCLUSIVE] Names, Ssn, Dl, Banking Info, Medical Recs.

Pages: 1 | 2 | 3 | 4 | Next

ImperialRussia — 2014-06-15 00:14:32 — #1

Member

From: Imperial Russia
Registered: 2014-04-07
Posts: 123

Store Grand Re-Opening!!!

Live and Exclusive database of US FULLZ from an insurance company, particularly from NorthWestern region of US. All fullz come in a .pdf format and contain 7-16 pages of very exclusive information, live from companies db. Most of the fullz come with EXTRA FREEBIES inside as additional policy holders.

[Name:]
[Address:]
[Phone #:]
[Driver License #:]
[SSN:]
[DOB:]
[Bank Name:]
[Routing Number:]
[Checking Account:]
[+ Draft date for their automated monthly payment.]
[Medical Records:]

All of the information is accurate and confirmed, Clients are from an Insurance Company database with GOOD to EXCELLENT credit score!

I, myself was able to apply for credit cards valued from $2,000 - $10,000 with my fullz.

Info can be used to apply for loans, credit cards, lines of credit, bank withdrawal, assume identity, account takeover.

BULK ORDER ONLY! 5 fullz = $40; 10 fullz = 70; 15 fullz = $110; 20 fullz = $140; 30 fullz = $210; 40 fullz = $280; 50 fullz = $320.
BULK ORDERS ONLY!!!

Ultima “moda”, vendere i “Fullz”, informazioni personali, bancarie, fiscali ecc. di una persona. Furti ma anche impersonificazione.
https://www.creditcards.com/glossary/term-fullz.php

In alcuni casi trovi anche il cognome della mamma da nubile o il nome del cane.
Valore sul mercato molto variabile.

Chi sono i “cattivi” ?

(Crypto)Kidnapper

Prende in ostaggio i dati dell’utente e chiede un riscatto.

Esempio di cattivo professionale molto attivo ultimamente.
Obiettivo: Prendere in ostaggio il PC o i dati dell'utente e chiedere un riscatto.
Tecniche:
Spingere l'utente a lanciare un applicativo infetto o a clickare su un link malevolo (normalmente sfruttando zero-day vulnerability).
Bloccargli il PC o cifrargli i file chiedendo un riscatto per sbloccarlo o per avere la chiave di decifratura.
Pagamenti in bitcoin.
Alcuni vecchi attacchi sono stati decrittati: https://www.nomoreransom.org/

Chi sono i “cattivi” ?

Ransomware – quanto rende?

Data	Campagna	Wallet	Bitcoin
29-11-2016 15-12-2016	stopper	1FwHxzFFGbAmmdkxhUUTEjocuDhEowDyuU	67.56167621
29-11-2016 20-12-2016	worm01	1KQhTbj9sGrQ596wBPZLQTpbiN1gBXwAny	28.53519378
10-12-2016 15-12-2016	mkgoro	1swAqc6dAyqcSaKdx8VnuJhhE9vaYLHFb	8.09468500
12-12-2016 15-12-2016	payforhelp	1GKpUP4SWC7TiiX7BkeST4i9bFNVyyPTjb	4.00000000
13-12-2016 16-12-2016	bitcoin143	19PuzW2WwD4jnhQLLvHun7cCeJq8HZux4	9.00000000
20-12-2016 21-12-2016	amagnus	1DaeQHLUbckx2tnshQrmcE45tEMB1UxjPS	4.00000000
07-01-2017 11-01-2017	bitcoin143	1AJa5kZY1LDzSLrYJ3SDq3CubX8qHwpjEN	12.50000000
05-01-2017 16-01-2017	cryptsvc	116CZ4y4mHs9ruzmYCufrwk4t17dsNEnAJ	26.00070000
		Totale Bitcoin	159.69225499

“Fonte: CRAM di TG Soft https://www.tgsoft.it”

Esempio di guadagni con una campagna di un mese e mezzo di Ransomware.

“Fonte: CRAM di TG Soft https://www.tgsoft.it ”

Chi sono i “cattivi” ?

Campagne mirate

Attacco hacker alla Bonfiglioli. "Chiesto riscatto di 2,4 milioni"

L'azienda decide di non pagare: "Abbiamo scelto di non assoggettarci al ricatto e non alimentare un meccanismo criminale"

Ultimo aggiornamento il **2 luglio 2019 alle 19:37**

Gruppo Iris, attacco hacker. Chiesti 950mila euro di riscatto

Due settimane fa il sistema dell'azienda è stato 'tenuto in ostaggio' Federica Minozzi: "Non abbiamo ceduto, i nostri tecnici hanno risolto tutto"

Ultimo aggiornamento il **28 dicembre 2018 alle 11:51**

Campagne mirate molto complesse.

Chi sono i “cattivi” ?

Danni collaterali (attacco NotPetya)

Logistica Maersk (**300M$**)

Chimica-farmaceutica Merck (**870M$**)

Logistica FedEx-TNT (**400M$**)

Industria Saint-Gobain (**384M$**)

Attacco NotPetya del 2017, sfugge di mano agli attaccanti (probabilmente) https://en.wikipedia.org/wiki/Petya_(malware)

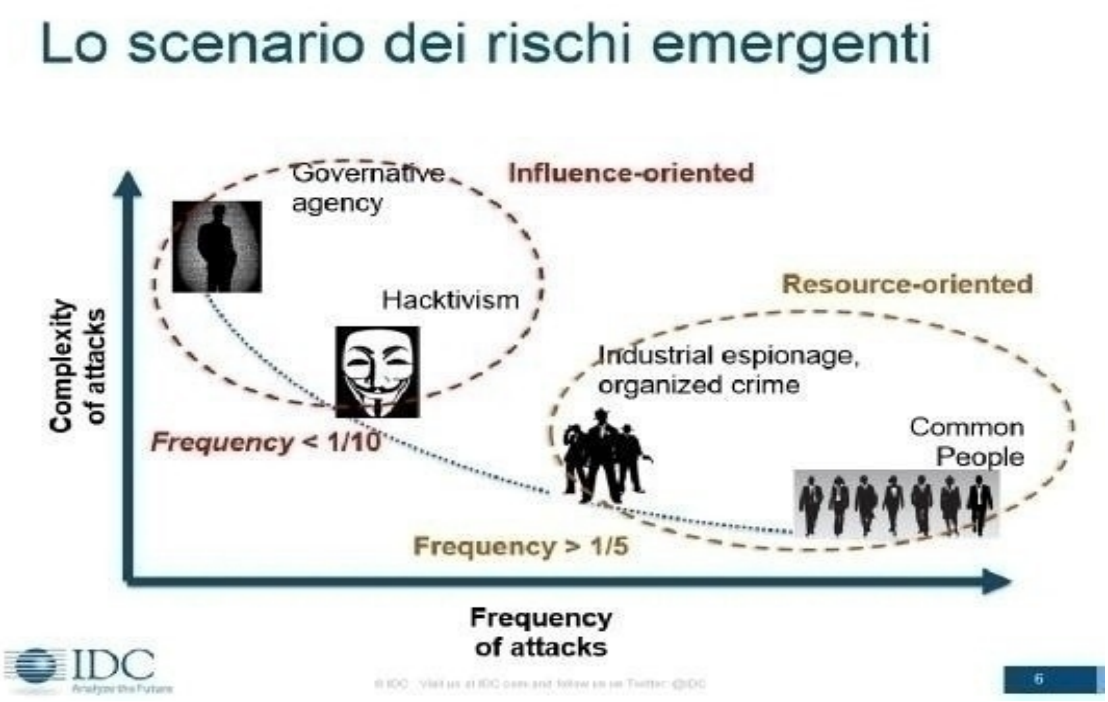
Chi sono i “cattivi” ?

Qualche consiglio per MITIGARE il rischio

- Antivirus
- Patch
- Plugin
- Browser+AD-blocker
- Backup
- Utenti non amministratori del PC
- Antivirus sulla posta
- Filtri di navigazione
- Bloccare cartelle sistema
- NO Windows Script Host

- Antivirus buono e sempre aggiornato
- Patch all'ultimo livello (soprattutto windows)
- Plugin aggiornati (Java, Adobe)
- Browser aggiornati con AD-blocker
- Backup protetti non in linea (e provare restore)
- Utenti non amministratori del PC
- Antivirus solidi sulla posta (Bloccare src,exe,com,vbs,js)
- Filtri aggiornati di navigazione
- Bloccare cartelle sistema con policy e permessi
- Disabilitare Windows Script Host

Chi sono i “cattivi” ?



Chi sono i “cattivi” ?

I cattivi-cattivi sono ESTREMAMENTE veloci e aggressivi

ANDY GREENBERG SECURITY 02.19.19 05:00 AM

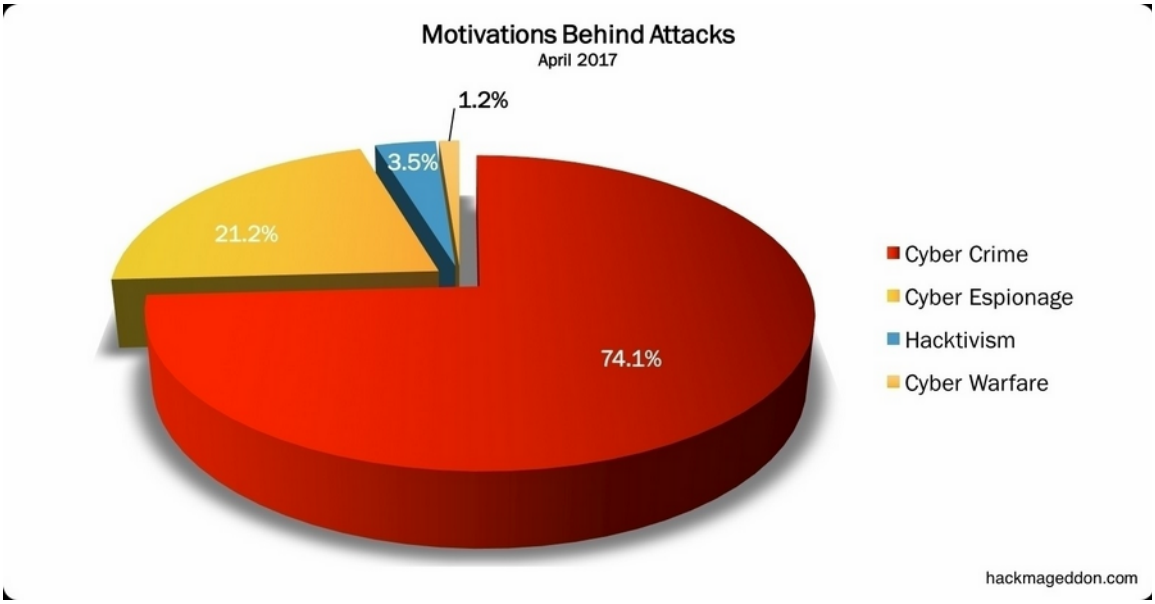
RUSSIAN HACKERS GO FROM FOOTHOLD TO FULL-ON BREACH IN 19 MINUTES

Dal primo punto di entrata (es. mail di phishing che viene aperta) al controllo come admin della rete in pochi minuti.

https://www.wired.com/story/russian-hackers-speed-intrusion-breach/

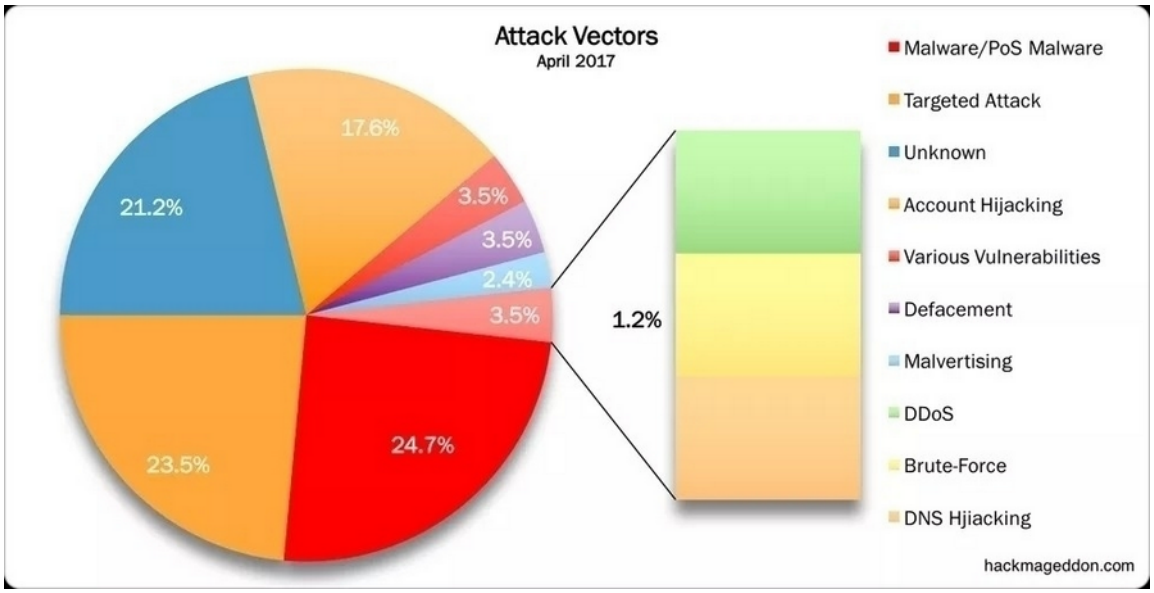
Analyzing more than 30,000 attempted breaches in 2018 CrowdStrike measured the time from hackers' initial intrusion to when they began to expand their access. Russia's hackers were far and away the fastest, expanding their access on average just 19 minutes. North Korea's hackers came next, averaging about two hours longer than the Russians. Chinese hackers took about four hours, Iranian hackers took more than five, and profit-focused cybercriminal hackers took nearly 10 hours.Doesn't include targets of hacking by the US, the UK, or the other English-speaking countries.

Chi sono i “cattivi” ?



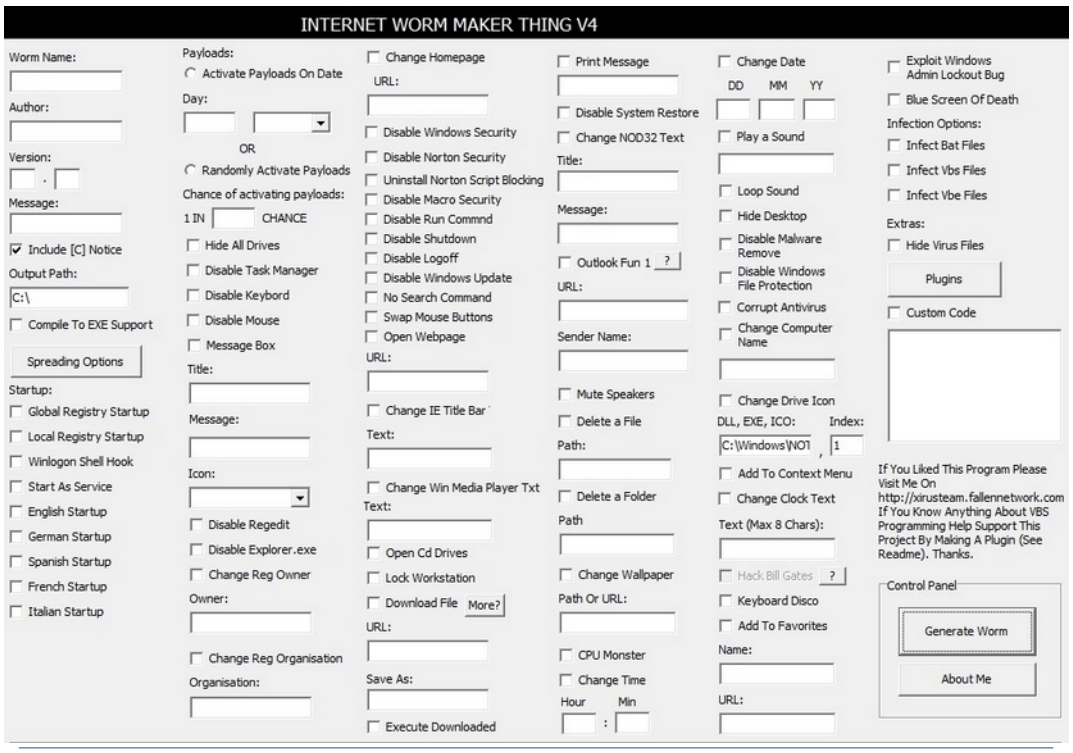
Fonte: http://www.hackmageddon.com/

Chi sono i “cattivi” ?



Fonte: http://www.hackmageddon.com/

Chi sono i “cattivi” ?



Non è difficile diventare “cattivi”, non serve nemmeno andare nel “Dark Web”, si trovano kit già pronti in rete per diventare “Script Kiddie”.
https://en.wikipedia.org/wiki/Script_kiddie

I principali tipi di attacchi

DOS - DDOS

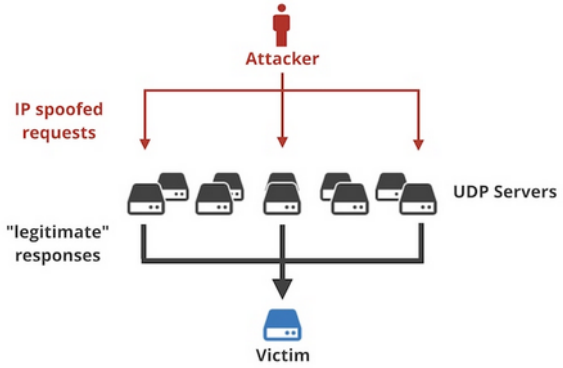
(agenti esterni o interni)

(Distributed) Denial of Service
https://en.wikipedia.org/wiki/Denial-of-service_attack
Impedire il funzionamento di un servizio con attacchi che possono partire anche da punti distribuiti della rete. Cui prodest?
Può essere un puro atto “vandalico” (Hacktivism), può servire per chiedere un riscatto oppure può essere il preludio di un altro attacco (blocco un servizio di difesa oppure blocco il servizio vero per attivarne uno falso).
Può essere fatto a diversi livelli (fisico, trasporto, applicativo, umano) anche algoritmico (mail bomb o pdf “complicati” ad esempio).
Acquistabile in service in rete: “the cost to power a DDoS attack using a cloud-based botnet of 1,000 desktops is about $7 per hour.”
http://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html

I principali tipi di attacchi

DOS - DDOS

Riflesso e amplificazione



Se non ho tanti attaccanti posso usare il metodo del riflesso e dell'amplificazione.
Ip spoofing del target poi richieste con poco input e tanto output di riflesso.
https://arstechnica.com/information-technology/2018/02/in-the-wild-ddoses-use-new-way-to-achieve-unthinkable-sizes/

DNS moltiplica per 50
NTP per 60
Protocollo memcache (cache db per web e reti) 50K

1.1Tbps di picco dell'attacco

Man in the middle
Connection hijacking

Man in the Middle attack
https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Può avvenire a vari livelli:
- Fisico (ethernet, wifi)
- Trasporto (TCP/IP)
- Applicativo (http)
- Umano (vedi “Social Engineering”)

Connection Hijacking: inserirsi all’interno di una conversazione oppure modificarne il flusso o i dati
Anche questo può avvenire a vari livelli.
E’ una generalizzazione del Man in the Middle.

I principali tipi di attacchi

Privilege Escalation
Buffer Overflow
Backdoor
Keylogging
IP Spoofing

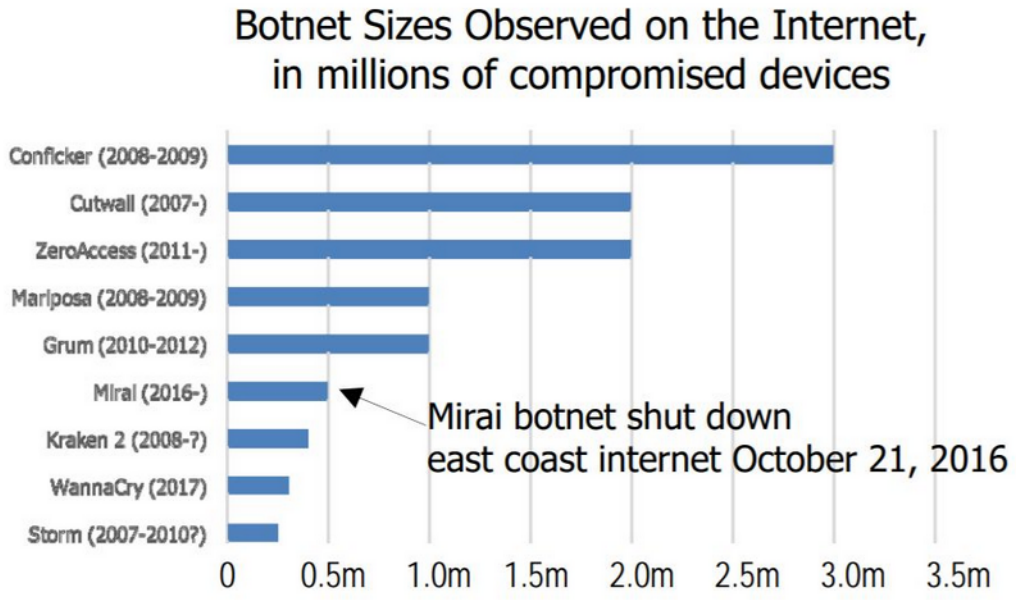
Privilege escalation: accedere ad un sistema/servizio con privilegi maggiori di quelli previsti per l'utenza. Sfrutta vulnerabilità, crash o errori di programmazione.
https://en.wikipedia.org/wiki/Privilege_escalation
Buffer overflow: accedere ad aree di memoria che non dovrei vedere. Lettura dati o esecuzione programmi.
https://en.wikipedia.org/wiki/Buffer_overflow
Backdoor: una porta di servizio ai miei sistemi/software di cui non sono a conoscenza. Errori di programmazione o lasciata volutamente (produttore, governi, criminali)
https://en.wikipedia.org/wiki/Backdoor_(computing)
Keylogging: intercettare i tasti che vengono premuti sulla tastiera, via software o hardware. Attacchi "over the shoulder".
https://en.wikipedia.org/wiki/Keystroke_logging
IPSpoofing: impersonificare un altro IP, sia per ingannare utente che per mettere in difficoltà l'IP spoofato
https://en.wikipedia.org/wiki/IP_address_spoofing

I principali tipi di attacchi

Command & control

Command & control
https://en.wikipedia.org/wiki/Command_and_control_(malware)
Termine di derivazione militare.
Rete di server che controllano macchine infette, zombie, botnet ecc.
Cercano di spostarsi velocemente (DNS) e utilizzano reti o macchine compromesse. A volte anche macchine reali ospitate in paesi “amici”.
Reti gerarchiche (multiserver) o P2P.
Utilizzano protocolli standard (IRC, TOR) e connessioni crittografate.
Difficili da tracciare e da fermare, richiedono un’organizzazione complessa dietro (governi, criminalità organizzata ecc.).

I principali tipi di attacchi



Command & control
https://en.wikipedia.org/wiki/Command_and_control_(malware)

Termine di derivazione militare.

Rete di server che controllano macchine infette, zombie, botnet ecc.

Cercano di spostarsi velocemente (DNS) e utilizzano reti o macchine compromesse. A volte anche macchine reali ospitate in paesi “amici”.

Reti gerarchiche (multiserver) o P2P.

Utilizzano protocolli standard (IRC, TOR) e connessioni crittografate.

Difficili da tracciare e da fermare, richiedono un’organizzazione complessa dietro (governi, criminalità organizzata ecc.).

I principali tipi di attacchi

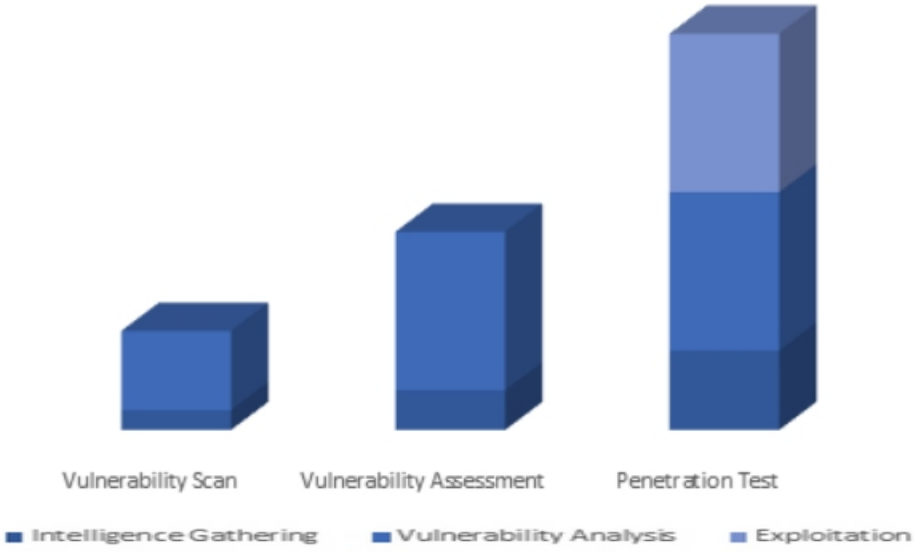
Advanced Persistent Threat

Advanced Persistent Threat
https://en.wikipedia.org/wiki/Advanced_persistent_threat

Identifica tutti gli attacchi che non mirano ad un risultato immediato ma sono complessi (Advanced) e mirano ad installarsi permanentemente nella rete dell'obiettivo (persistent) facendo movimenti orizzontali. Solitamente esfiltrano dati per lungo tempo oppure rimangono nascosti fino al momento di "esplodere".

I principali tipi di attacchi

Analisi preventive



Analisi preventive (audit)

- Scansione = raccolta di informazioni (automatico)
- Assessment = consolido i dati e verifico se ci sono falsi positivi (ad. es.) (semi automatico)
- Penetration test = provo a fare l'exploit delle vulnerabilità e ad entrare effettivamente nei sistemi (richiede operazioni manuali e conoscenza dei sistemi target)

Video interessanti di storie vere di pen-tester:
https://www.rapid7.com/info/under-the-hoodie/

I principali tipi di attacchi

(U) Table 1. Security Weaknesses Identified at [redacted] Facilities Visited

Unclassified Security Weakness	Facility Visited*				
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Multifactor Authentication Was Not Consistently Used	X		X		X
Network Vulnerabilities Were Not Consistently Mitigated	X	X			X
Server Racks Were Not Consistently Secured	X			X	
Data on Removable Media Was Not Consistently Protected and Monitored		X	X	X	
Intrusion Detection Was Not Implemented			X		
Administrators Did Not Require or Maintain Justification for Access	X	X	X	X	X
Physical Security Controls Were Not Implemented			X	X	X **Unclassified**

*(U) The [redacted] maintained separate facilities for administrative activities at the [redacted]. Therefore, checkmarks in those columns could indicate issues at either an administrative facility, a lab, or both. For details, see the discussion section of this report.

Source: The DoD OIG.

Esempio di output di audit.
In questo caso si tratta della verifica della sicurezza del sistema di controllo dei missili nucleari balistici degli Stati Uniti. :-O

https://www.zdnet.com/article/us-ballistic-missile-systems-have-very-poor-cyber-security/

Fasi dell'attacco

- Raccolta informazioni (Sniffing, Port Scanning oppure OSINT)
- Raccolta/costruzione armi
- Spedizione carico maligno o intrusione
- Sfruttare il carico maligno o l'intrusione
- Installare persistenza (APT)
- Command & control
- Azioni su obiettivo

Preparare un attacco: prima fase raccolta di informazioni.

Sniffing (packet analyzing) https://en.wikipedia.org/wiki/Packet_analyzer raccolta di dati sul tipo e contenuto del traffico. Utile anche come strumento di Problem Determination. (Wireshark)

Port Scanning https://en.wikipedia.org/wiki/Port_scanner raccolta di informazioni su un host, servizi usati, livelli di software, vulnerabilità ecc. Molto utile ma espone al rischio di essere scoperti. (Nmap)

I principali tipi di attacchi

Kill Chain militare

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and control
7. Action on objectives

1. Reconnaissance: ottenimento di informazioni sulla vittima
2. Weaponization: creazione del payload malevolo (exploit/documento/malware) che sarà usato per compromettere la rete del cliente
3. Delivery: invio del payload alla vittima. Nel caso di un’azienda la vittima può essere un particolare utente ritenuto vulnerabile.
4. Exploitation: esecuzione del payload malevolo sulla vittima
5. Installation: persistenza del malware o dell’attaccante all’interno della vittima.
6. Command and control: instaurazione della connettività con il centro di controllodel malware.
7. Action on objectives: esecuzioni di azioni per il raggiungimento dell’obiettivo, come esfiltrazione dati o propagazione orizzontale.

Damage Control

E durante l'attacco cosa faccio?

Se sono sotto attacco intendo

Damage Control

E durante l'attacco cosa faccio?

E durante l'attacco cosa faccio?
"Damage control" (termine di derivazione navale che vuol dire: "darsi da fare per non far affondare la nave che imbarca acqua").

- Mettere in sicurezza i dati
- Fare la conta dei danni
- Pianificare azioni di ripristino
- Comunicare (interno, esterno, clienti, fornitori, stakeholders)
- Capire come è successo e di conseguenza attrezzarsi in modo che non succeda più

Damage Control

Israel Defense Forces
@IDF
Segui

CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed.

Traduci il Tweet

Contrattaccare è illegale.
(anche lanciare missili contro il datacenter dell'attaccante sarebbe da evitare)

Damage Control

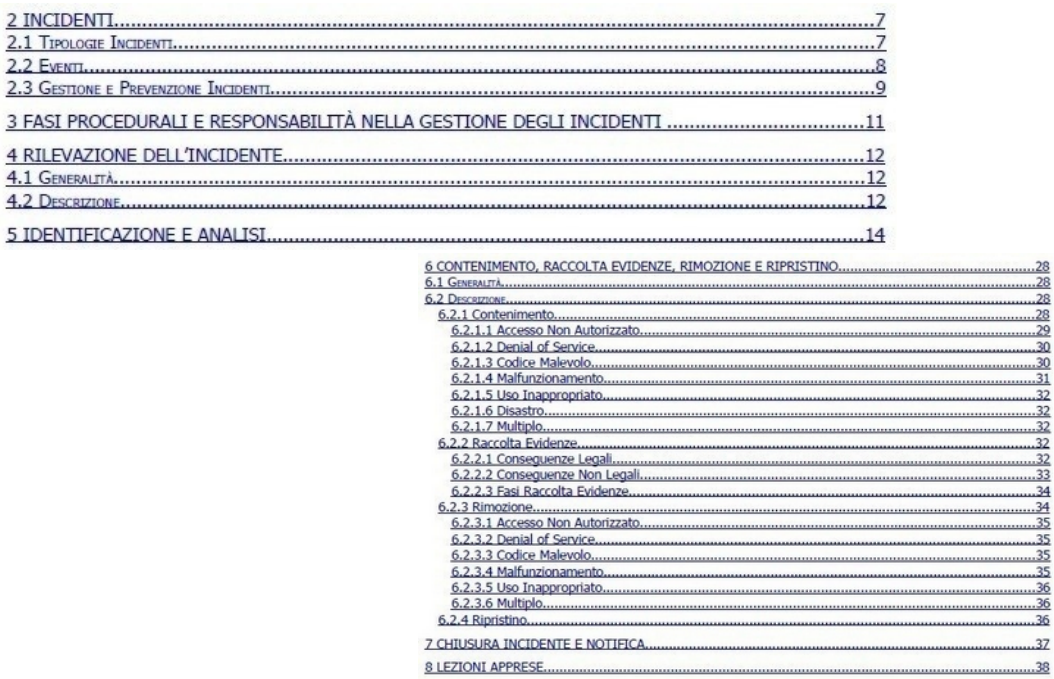
Piano per la gestione degli incidenti informatici

(aggiornato, conosciuto, accessibile, condiviso, unico ...)

Avere un responsabile del piano (o una gerarchia).
Elencare i rischi, le minacce e i potenziali incidenti.
Sviluppare guide rapide per gli scenari più probabili.
Stabilire procedure per prendere le decisioni più importanti.
Modalità di rapporto con i principali interlocutori esterni.
Avere contratti di servizio e con fornitori ed esperti.
Tenere aggiornata e disponibile la documentazione.
Assicurarsi che tutti abbiano chiari i propri ruoli e responsabilità.
Identificare gli individui che sono fondamentali per la risposta agli incidenti e garantire la ridondanza.
Fare simulazioni di incidente e raffinare i piani di conseguenza.

Attenzione! Con la nuova normativa Europea diventa obbligatorio averlo. Segnalare incidente entro 72 ore se coinvolge dati personali.

Damage Control



Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna

Damage Control

Incident Response Team

- IT and security teams
- Outside consultants
- Executive management
- Compliance/Legal
- Business operations
- Human resources
- Public relations/External Communication
- Vendors/Business partners

- IT and security teams
- Outside consultants: se serve competenza extra
- Executive management: per prendere decisioni strategiche (spengo la produzione per x minuti)
- Compliance/Legal (GDPR, eventuali certificazioni, rischi legali del data breach per l'azienda, rischi di azioni da intraprendere)
- Business operations (chiudo il portale ordini, comunicare in azienda)
- Human resources (mi serve quella persona che lavori tutta la notte, comunicazione in azienda, violazione policy)
- Public relations (comunicazione all'esterno, **le parole della crisi (esempio FFSS e il treno "sviato" a Pioltello)**)
- Vendors Business partners (ISP, hw e SW vendor, app vendor ecc.)

Digital Forensics

http://en.wikipedia.org/wiki/Digital_forensics

L'anatomo patologo del mondo digitale.
Fondamentale per avere delle prove valide in un processo per un crimine informatico.
Non bisogna contaminare la scena del crimine (ad esempio non spegnere uno smartphone ma metterlo in modalità “aereo” http://www.bbc.com/news/technology-29464889 per evitare brutte sorprese).
Garantire autenticità e affidabilità dei dati recuperati dai dispositivi (ove possibile con riproducibilità delle operazioni). Scientificità in tutte le fasi di gestione dell'«evidenza». Conoscere le debolezze della tecnologia su cui si sta operando e scegliere la migliore soluzione caso per caso.

Digital Forensic

Magari non mi presento da un giudice con dei dati estratti da un iPhone con un dispositivo da 230€ cinese comperato online ...

http://www.ebay.it/itm/IP-BOX-APPLE-iPAD-iPHONE-2G-3G-4-4S-5-5C-5S-iOS8-1-PASSWORD-UNLOCK-TOOL-IPBOX-/131475790206

Cosa può aver fatto ai dati del mio telefono quel dispositivo non è dato a sapere per cui la prova, a livello legale, non è più valida (ma le informazioni se mi servono ce le ho …).
Nota: **AL MOMENTO** il dispositivo **disponibile su eBay** non funziona con gli ultimissimi iPhone.

Digital Forensic

Ma si trovano anche rivenditori ufficiali.

Cellebrite Rugged PRO

Ad esempio i prodotti Cellebrite
https://www.cellebrite.com/en/platforms/
Nuovo 6000$, c'è chi l'ha trovato usato e pieno di dati su E-bay per 100$
https://www.forbes.com/sites/thomasbrewster/2019/02/27/the-feds-favorite-iphone-hacking-tool-is-selling-on-ebay-for-100and-its-leaking-data/#5a2f732f5dd4
Israeliani ma sponsorizzati dagli USA
https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/#365793b0a1fc

CELLEBRITE SAYS IT CAN UNLOCK ANY IPHONE FOR COPS
https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/

Digital Forensic

La storia curiosa di una indagine, parlando di gatti, macchine e telefoni:
The Koobface malware gang – exposed!

https://nakedsecurity.sophos.com/koobface/
Koobface=importante attacco Malware con un meccanismo di Command e Control

Digital Forensic

Command&control srv → statistiche → file corposo → backup → sorgenti →

- Numeri di telefono → Russia
- Immagine → exif → San Pietroburgo
- Nickname → annunci online
  - Gatti → email e nickname
  - Auto → numero di targa

email+nickname → Facebook (profilo bloccato e nome fittizio ma c'è la fotografia, e gli amici, non bloccati, la moglie) → immagini della macchina corrente, della casa, del luogo di lavoro → nome dell'azienda → sede a San Pietroburgo → ricerca sui social dei dipendenti → immagine corrisponde → abbiamo nome, faccia, telefono, mail ecc.

La prossima ricerca potresti essere tu ...

https://nakedsecurity.sophos.com/koobface/
Koobface=importante attacco Malware con un meccanismo di Command e Control

Semplificazione dei passaggi, per il dettaglio con tutti gli screenshot vedi documento sophos_koobface_article.pdf

Honeypots

https://en.wikipedia.org/wiki/Honeypot_(computing)

Honeypot: vaso di miele per attirare gli attaccanti, può servire per studiare gli attacchi oppure per distrarre l'attaccante. Ambienti simili alla produzione ma innocui e isolati. Es. Caselle di posta predisposte per attirare lo spam. Si può valutare un attacco in corso

By aussiegall from sydney, Australia (Old Honey Pot) [CC BY 2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons

Sandbox

https://en.wikipedia.org/wiki/Sandbox_(computer_security)

Sandbox: buca di sabbia dove far esplodere le bombe. In input ci appoggio le mail sospette prima di recapitarle al destinatario e simulo le azioni che farebbe l'utente per vedere cosa succede (se esplode). Se uso personal mail mi serve una personal sandbox.

In uscita (proxy navigazione) posso testare i link dubbi e vedere cosa fanno (rallenta la navigazione).

Canary

https://canary.tools/
Canary: appliance che fanno scattare allarme quando sono compromesse. No analisi, solo allarme. Più semplice da gestire di Honeypot. (canarini nelle miniere)

http://docs.opencanary.org/ (open source)

Fino a veri e propri sistemi di emulazione di reti aziendali in grado di gestire trappole complesse:
https://en.wikipedia.org/wiki/Deception_technology
Nova (open source) http://www.projectnova.org genera reti e host fittizzi che fanno perdere tempo all'attaccante.

Sono tutti elementi di difesa attiva (legale, contrattacco=illegale)

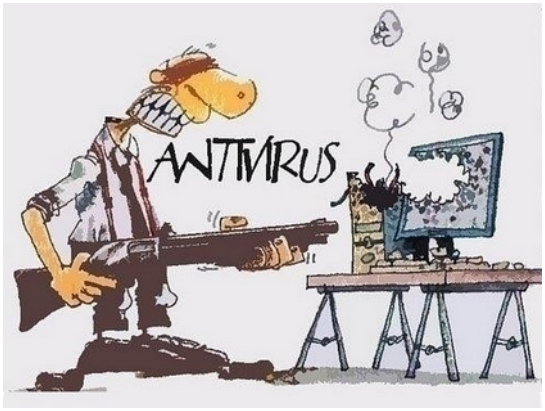
Il bersaglio

Il bersaglio

Il bersaglio solitamente parte dal presupposto di non essere tale. Sindrome del “perchè dovrebbero attaccare proprio me”.

Magari perché non sei tu il bersaglio reale ma servi solo come “sponda”.

Modello mentale



vs

Capire i meccanismi mentali e i modelli che l'utente si costruisce rispetto ai potenziali strumenti di attacco.
Perché una tecnologia funzioni bisogna che il modello della minaccia sia percepito allo stesso modo da chi sviluppa il software e da chi lo dovrà utilizzare (esempio del lucchetto per https e del “cestino” di Windows).
Attenzione all'influenza dei modelli culturali di base (occidentale/orientale, giovane/anziano ecc.).

Il nemico

Il nemico

Il “nemico” non è sempre “fuori”, non è sempre cattivo e a volte non sa nemmeno di essere “il nemico”.

E allora perché diventa un “nemico”?

E' importante capire i meccanismi perché sono più complessi di quelli dei nemici naturali esterni.

Come abbiamo visto in precedenza i nemici esterni solitamente sono “cattivi di professione”.

Capire i meccanismi per prevenire i comportamenti ostili, sbagliati o semplicemente dannosi del nemico “interno”.

La consapevolezza del gesto criminale

Realtà esterna + esperienza personale/collettiva
→ Atteggiamenti diffusi + percezione sociale
→ Elaborazione mentale + calcolo pro/contro
→ Scelta del comportamento/azione

La consapevolezza del gesto criminale

Le persone, prima di commettere un illecito, valutano i pro e i contro e le conseguenze del loro gesto. Percepiscono, valutano, pensano; poi decidono se agire o no.

L'essere umano orienta il proprio comportamento (a maggior ragione quello criminale) in base ad una serie di informazioni che provengono dalla sua esperienza e dall'ambiente esterno.

Realtà esterna + esperienza personale/collettiva
→ Atteggiamenti diffusi + percezione sociale
→ Elaborazione mentale + calcolo pro/contro
→ Scelta del comportamento/azione

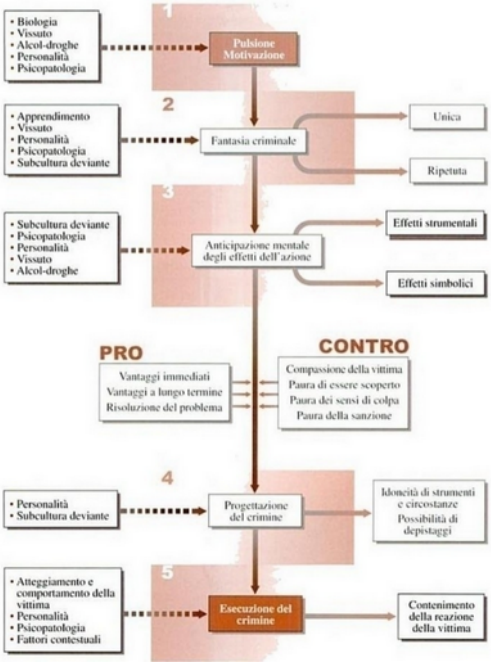
La consapevolezza del gesto criminale

1) Motivazione/pulsione a compiere l'azione
2) Fantasia criminale
3) Anticipazione mentale degli effetti dell'azione
4) [eventuale] Progettazione del crimine
5) [eventuale] Esecuzione del crimine

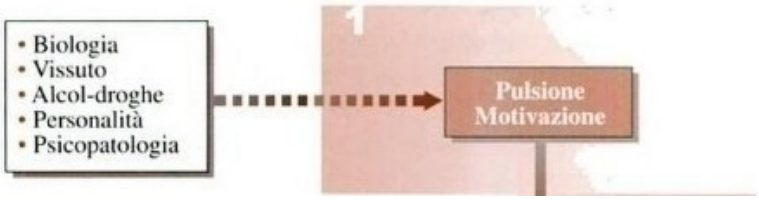
La dinamica criminale secondo il Prof. Marco Strano (Manuale di Criminologia Clinica) è articolata in cinque fasi di pensiero che inconsciamente si susseguono nella nostra mente:

1) Motivazione/pulsione a compiere l'azione
2) Fantasia criminale
3) Anticipazione mentale degli effetti dell'azione (empatia con la vittima, sensi di colpa, rischio di essere scoperto, possibilità di essere denunciato una volta scoperto, paura della sanzione, cosa ne pensa "il branco" ecc.)
4) [eventuale] Progettazione del crimine
5) [eventuale] Esecuzione del crimine

Cenni di criminologia

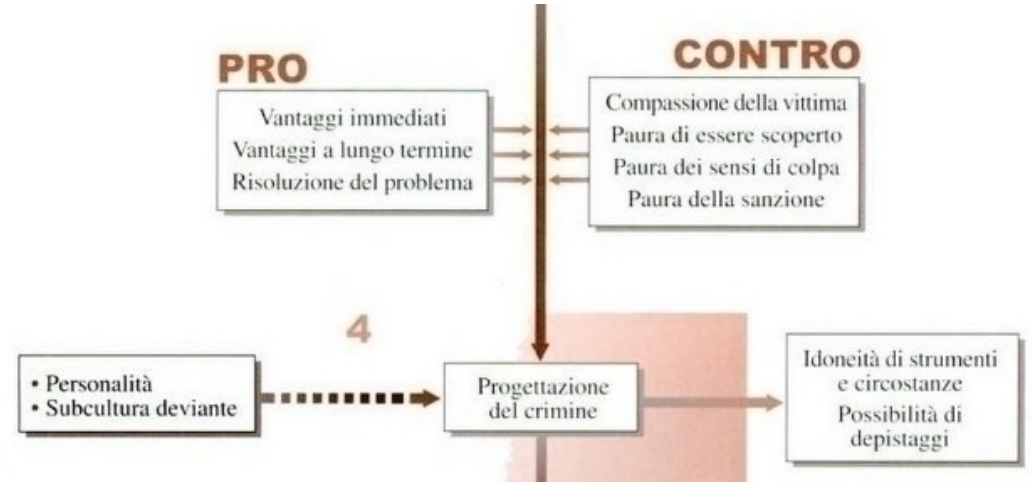


Cenni di criminologia



Cenni di criminologia

Cenni di criminologia




• Atteggiamento e comportamento della vittima
• Personalità
• Psicopatologia
• Fattori contestuali
5
Esecuzione del crimine
Contenimento della reazione della vittima

L'intermediazione tecnologica del gesto criminale

L'intermediazione tecnologica del gesto criminale.

Nel “computer crime” scompare il contatto fisico fra l'autore del reato e la vittima.
A volte scompare anche il contatto fisico fra il reato e l'oggetto del reato.
Questo cambia completamente la fase di anticipazione mentale del crimine.
Anche il rapporto empatico con la potenziale vittima ne viene ovviamente influenzato.

L'intermediazione tecnologica del gesto criminale

- Percezione degli effetti
- Possibili autori di reato
- Illegalità distribuita
- Senso di impunità
- Disaccoppia le leggi dall'azione criminale

- Attenua la percezione degli effetti del crimine sulla vittima
- Allarga la base dei possibili autori di reato rendendo adatti al crimine anche soggetti normalmente estranei al mondo della criminalità tradizionale
- Crea un fenomeno di illegalità distribuita in larghe aree sociali (vedi ad esempio il tema della violazione dei diritti d'autore o della copia illegale del software)
- Diffonde un falso senso di impunità su determinati crimini (spesso solo per mancanza di informazione)
- Disaccoppia le leggi civili e penali dall'azione criminale in corso (vengono vissuti come due “mondi” diversi)

Per approfondimenti: http://www.criminologia.org/

Come incassare i proventi illeciti:
Bitcoin (di per sé lecito)

https://en.wikipedia.org/wiki/Bitcoin

Arriviamo al bitcoin partendo da Blockchain (libro mastro delle transazioni) non sono la stessa cosa ma sono collegati.

Cosa è Blockchain?

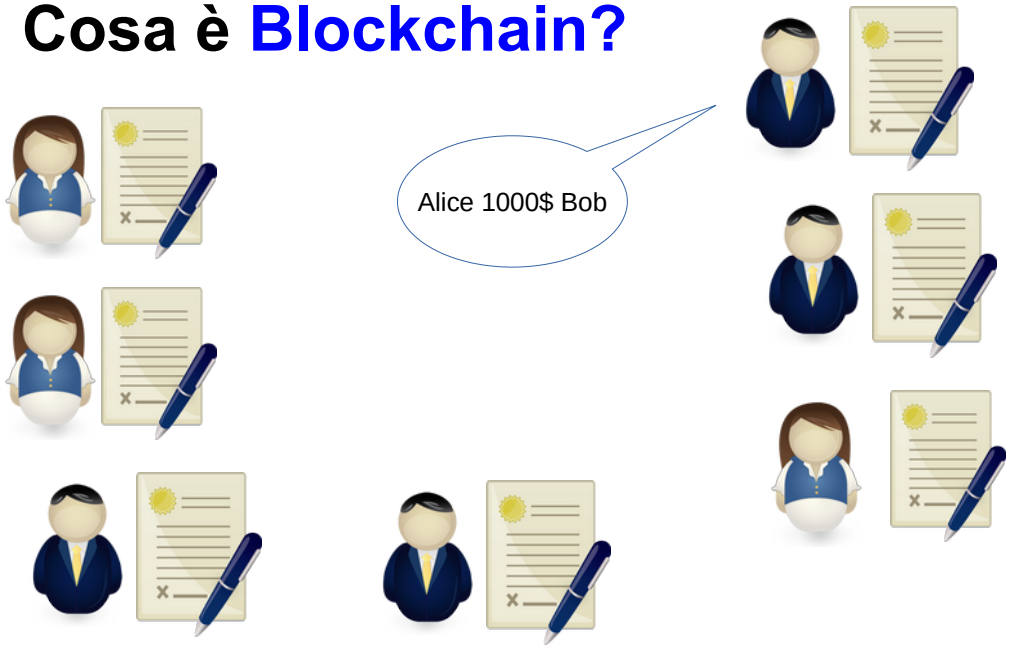
https://en.wikipedia.org/wiki/Blockchain

Nelle transazioni tradizionali ci si appoggia alla banca per trasferire denaro. Alice deve dare 1000$ a Bob, lo dice alla banca che segna la transazione sul libro mastro. Non si muovono fisicamente soldi.

Problemi:

- Ci si deve fidare della banca
- Potenziali errori
- Potenziali irregolarità
- E se la banca perde il registro?

Cosa è Blockchain?

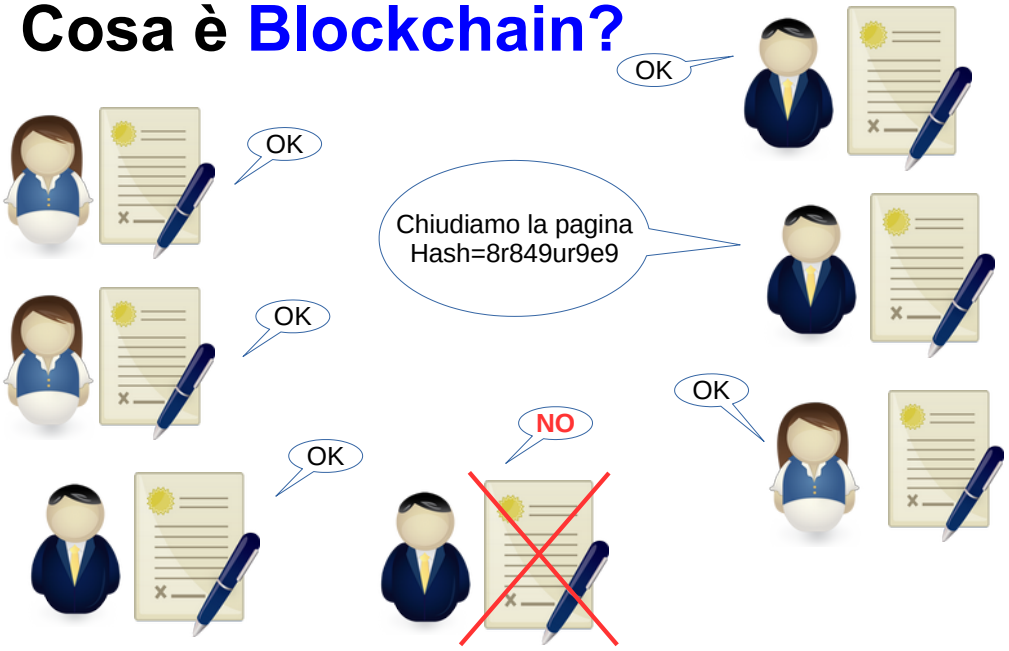


Blockchain è un libro mastro distribuito dove in tanti tengono traccia delle transazioni, ognuno annuncia le sue transazioni e tutti le scrivono.

Il libro mastro virtuale ha lo stesso numero di “righe per pagina” per tutti per cui dopo un certo numero di transazioni tutti riempiono la pagina assieme.

Bitcoin

Cosa è Blockchain?



Chiudere la pagina significa calcolare hash (azione di "Mining").

Quando la pagina è "piena" tutti si mettono a calcolare l'hash, il primo che finisce annuncia il risultato.

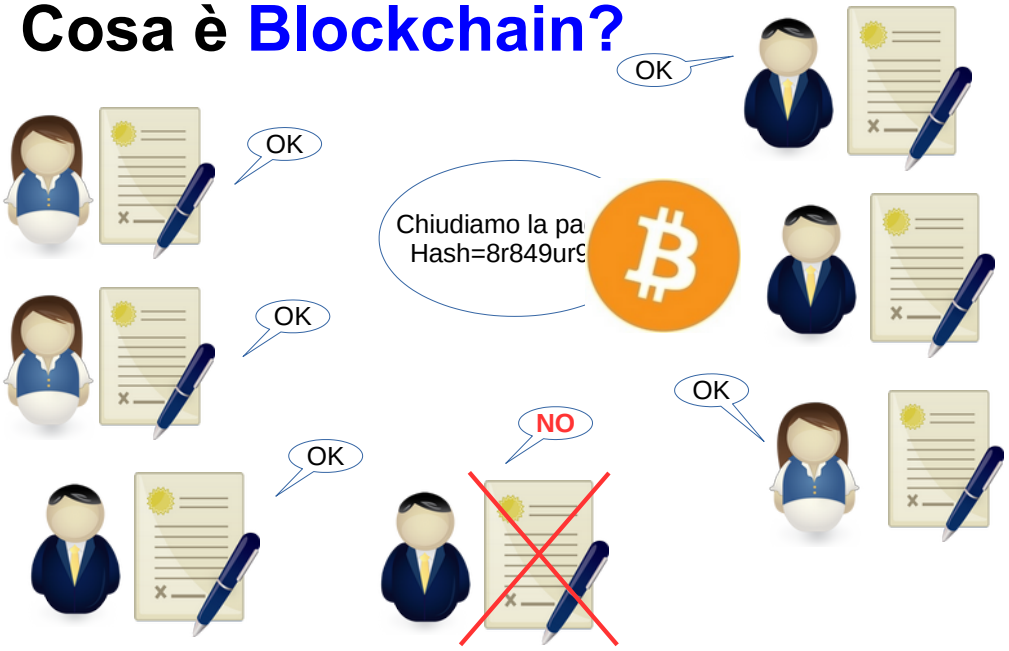
Se tutti abbiamo fatto bene l'hash è uguale per tutti e la pagina a questo punto è sigillata con il suo hash, memorizzata da tutti i partecipanti e non più modificabile.

Se uno ha scritto male qualcosa ottiene un hash diverso e deve sostituire la pagina con una di quelle buone.

Per creare la "catena" di pagine in realtà l'hash viene calcolato tenendo conto anche dell'hash della pagina precedente in modo da evitare modifiche ad una pagina isolandola.

Pagina=blocco, catena di pagine=blockchain

Cosa è Blockchain?



Chi ha finito il “mining” per primo riceve un premio in Bitcoin (12/2017 premio = 12.5B, dimezza ogni 4 anni per arrivare a zero e fermare produzione)

Questi Bitcoin nascono dal nulla, non è che il premio che prende lui esce dal borsellino di un altro, è un “nuovo” Bitcoin.

Tanti vantaggi (libro mastro distribuito, catena delle transazioni protetta ecc.).

Attaccabile se il 51% delle persone diventano disoneste (improbabile ma non impossibile).

Altro meccanismo di reward=fee associato a transazione, viene scritta nel blocco quella che offre di più, le altre aspettano.

7/2019 circa 200.000 miner nel mondo

Nota: hash SHA-256 con valore casuale aggiunto, vince chi trova il valore che produce Hash più basso.

Grandi potenzialità di Blockchain in ambito sicurezza

Ovviamente questa disintermediazione delle transazioni crea qualche problema “politico”.
Tecnologia che nasce assieme a bitcoin ma ora vive vita propria per molti altri usi.
La natura blindata e distribuita di Blockchain potrà dare grandi contributi in ambito sicurezza.
Implementazioni di sistemi PKI senza bisogno di una CA centralizzata (CertCoin MIT https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf)
Protezione dalla manipolazione dei dati, hash dentro a blockchain (Guardtime per governo Estone https://guardtime.com/blog/blockchain-enabled-cloud-estonian-government-selects-ericsson-apcera-and-guardtime)
Gestione contratti = Smart Contracts
Gestione password (Remme https://www.remme.io/)

Potenziali problemi

- Transazioni/sec
- Dimensioni chain
- Consumo corrente elettrica
- Transazioni irreversibili

Potenziali problemi (ad oggi 12/17):

- 3-4 transazioni al secondo (Visa 60K) giorni per avere una transazione convalidata. Migliorabile aumentando dimensione del blocco ma poi più potenza di calcolo richiesta ai miner, meno miner= meno sicurezza.
- La chain cresce all'infinito e se voglio fare smart contrats debbo pensare anche agli allegati (2/19 200GB blockchain dei bitcoin, cresce circa 4GB/mese)
- Mining dei bitcoin assorbe energia elettrica come tutto l'Equador
- Transazioni irreversibili, è un bene ma anche un male (reso prodotti?)

Complessità hash calcolata per tenere 6 blocchi all'ora, blocco=1M, transazione 500B, 2K transazioni a blocco, circa 3-4 transazioni al secondo

Varianti

- Bitcoin Cash
- Bitcoin Gold
- Lightning

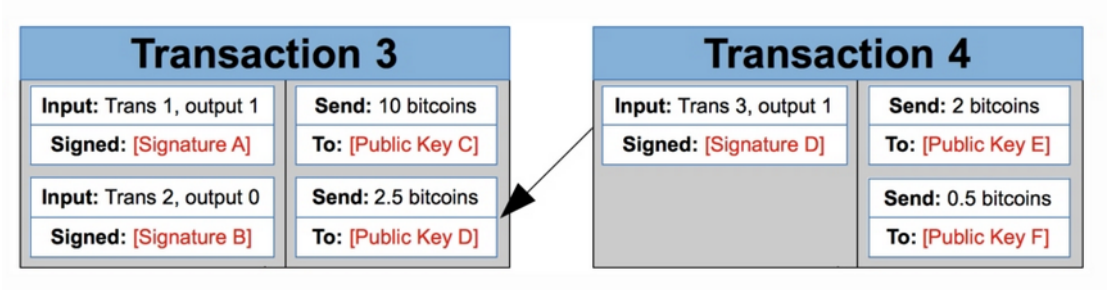
- Cambio dimensione del blocco=fork della catena. Bitcoin cash=blocco 8MB invece di 1MB
- Bitcoin Gold con algoritmo di mining più semplice per ricreare un ambiente realmente distribuito (CPU e non GPU)
- Lightning crea canale diretto fra compratore e venditore per piccole somme (more or less)

Cosa è Bitcoin?

- Rete di pagamento digitale ideata nel 2009 da “Satoshi Nakamoto” (anonimo), basata sulla crittografia (“crittovaluta”): algoritmo di firma digitale asimmetrica e algoritmi di hashing
- **Peer to peer, nessun ente centralizzato**
- Controvalore in valuta stabilito dal mercato
- **Possesso e trasferimento anonimo della valuta**
- Portafoglio digitale personale
- Blockchain=libro mastro delle transazioni=distribuito

https://en.wikipedia.org/wiki/Bitcoin

Esempio transazione



Ogni transazione prende un input di bitcoin da un’altra transazione e li trasferisce in output alla chiave pubblica di qualcuno.

Se sono D, con la mia chiave privata recupero l’output della transazione 3 e trasferisco a E e F i bitcoin.

Ogni transazione n input e m output ma debbo trasferire tutti i bitcoin, magari di nuovo a me stesso (oppure il resto lo uso per ricompensare i miner che mi fanno “passare avanti”.

L’indirizzo del destinatario (del suo wallet) è un hash della sua chiave pubblica.

Linguaggio di script per mettere vincoli (firme multiple, incassare non prima del, ecc.)

Bitcoin

1 bitcoin=11.000€ a luglio 2019

https://localbitcoins.com/

https://bitcoinity.org/markets