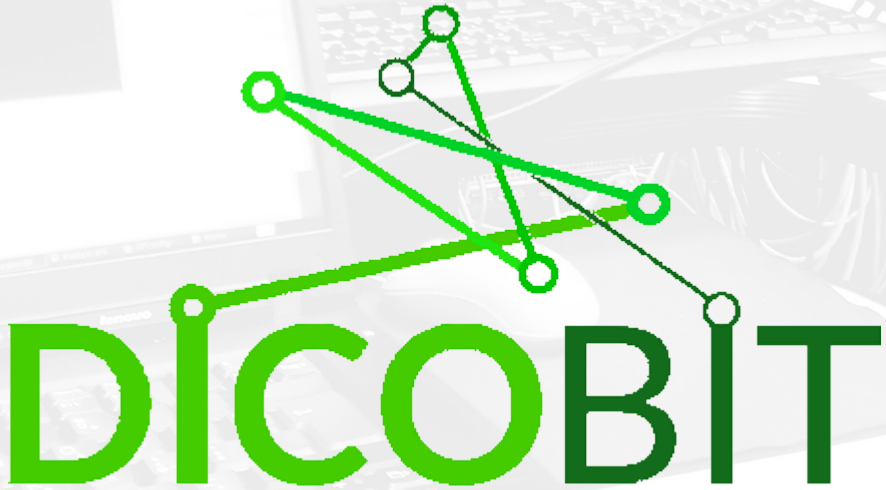
Linux Day
27 ottobre 2018

Spam
dalla pubblicitá ai criptolocker

Massimo Nuvoli

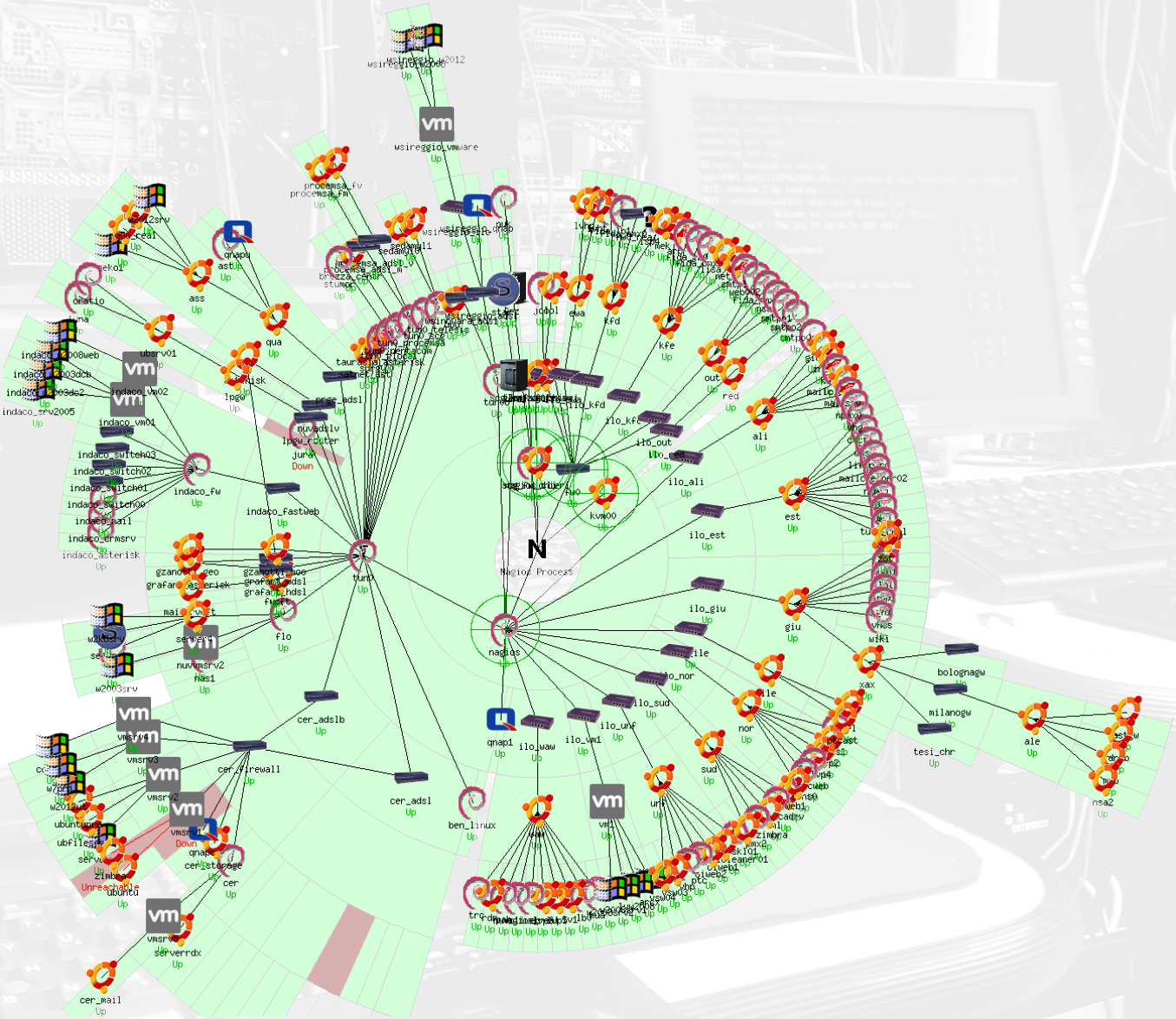
Chi sono?

- Sistemista “Architetto di Sistemi”
- Amministratore delegato di Progetto Archivio SRL Dicobit
- Consulente Tecnico in ambito legale
- Mi occupo di SPAM da 20 anni

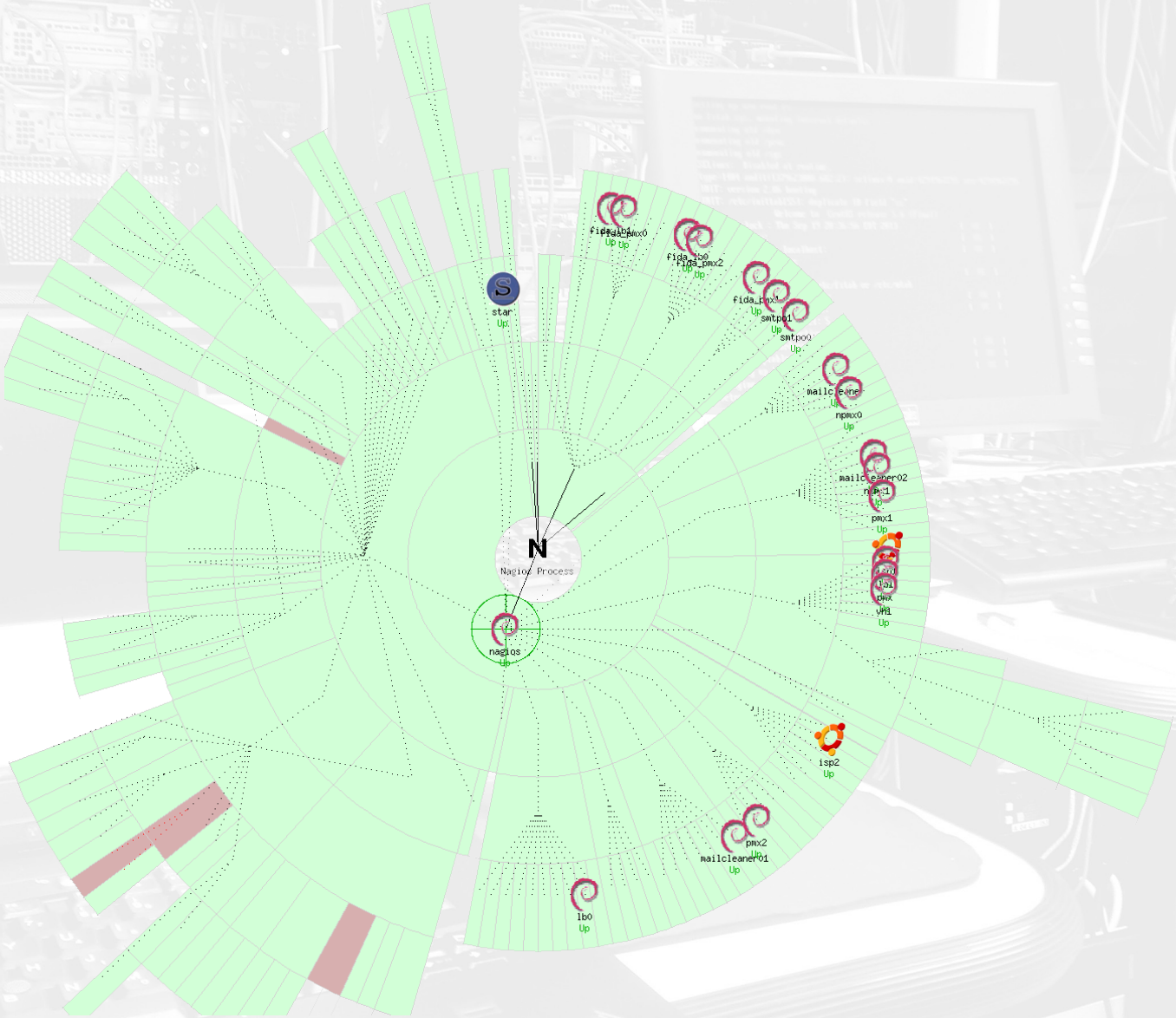


Ma anche..

La nostra struttura



La posta nella nostra struttura



Cosa significa?

- Spam = Junk email ovvero spazzatura
- Spam in realtá é la marca di un prodotto in scatola

Un po' di storia: anno 1978

- Il primo messaggio classificato come spam é del 1978, mandato a 600 destinatari
- Immediatamente la rete (in quel momento poco diffusa) comprende i limiti di smtp aperti e inizia a dare delle policy
- In questo periodo smtp é “aperto”

Anni '90

- Lo spam diventa “business” e cresce di dimensioni
- Cresce la lotta, iniziano le modifiche alle policy
- Smtp deve essere piú controllato
- Inizia la (fallimentare) richiesta normativa contro lo spam

Anni '00

- Cresce lo spam e cresce la lotta tecnologica
- Inizia finalmente (almeno in Europa) la lotta a livello legislativo
- Ovviamente noi italiani...

Oggi

- Dopo il 2000 le cose peggiorano
- Rientrano nello Spam trojan worm e cryptolocker che usano la posta per diffondersi
- La “qualitá” dei messaggi aumenta
- Dopo picchi ben al di sopra ora siamo ad un 55% circa di email spam sul totale nel mondo

Cosa dice la legge oggi?

- Non tutto lo spam é illegale!
- Con il GDPR serve il consenso per mandare email commerciali a chiunque, e ci sono pesanti sanzioni
- Le sanzioni per chi viola le disposizioni di legge vanno dalla "multa", in particolare per omessa informativa all´utente (fino a 90mila euro); alla sanzione penale qualora l´uso illecito dei dati sia stato effettuato al fine di trarne per sé o per altri un profitto o per arrecare ad altri un danno (reclusione da 6 mesi a 3 anni). E´ prevista anche la sanzione accessoria della pubblicazione della pronuncia penale di condanna o dell´ordinanza amministrativa di ingiunzione.

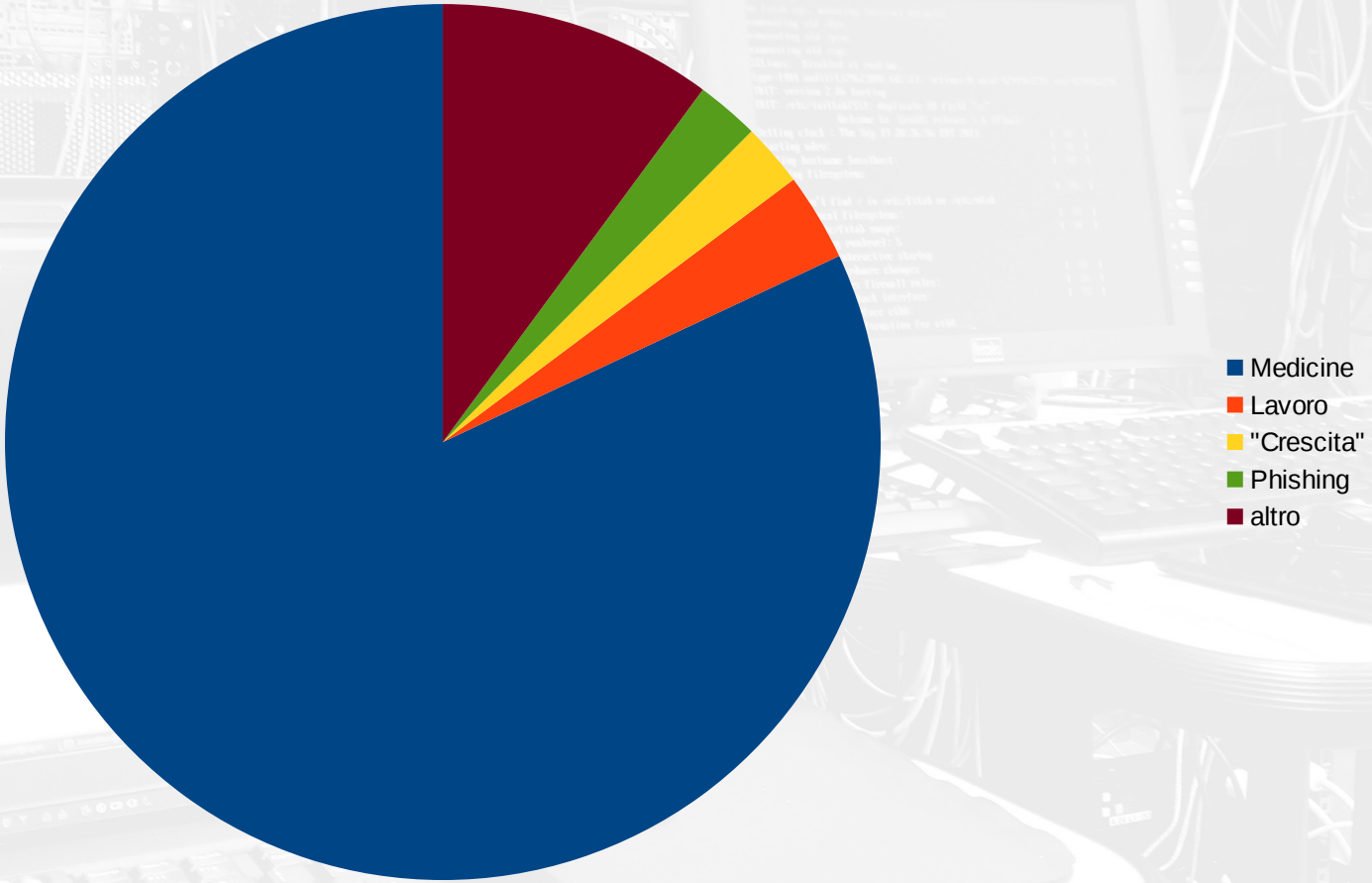
Ok in Italia ma il resto del mondo?

- Solo in questi giorni anche gli USA iniziano a pensare a qualcosa di simile al GDPR, un po' per la privacy, un po' perché si sono resi conto che tutto quanto sta diventando molto molto pericoloso
- Nel mondo non esiste una legislazione uniforme, difatto basta andare in uno stato deregolamentato per mandare spam e non essere perseguibili
- Alla fine gli strumenti “tecnici” restano l'unica strada per limitare l'illegalitá

Qual é il maggior rischio?

- **Dati correlati!**
- Se sai nome e cognome, indirizzo email, magari una vecchia password, e qualche dato personale hai una superficie d'attacco migliore
- Se hai delle comunicazioni intercorse e puoi usarle per farne una piú verosimile l'attacco é ancora piú potente
- In tutti questi casi si presenta la perdita incontrollata di informazioni che é pesantemente punita dal GDPR e che molti ancora ignorano

Statistiche pubblicitá (2010)



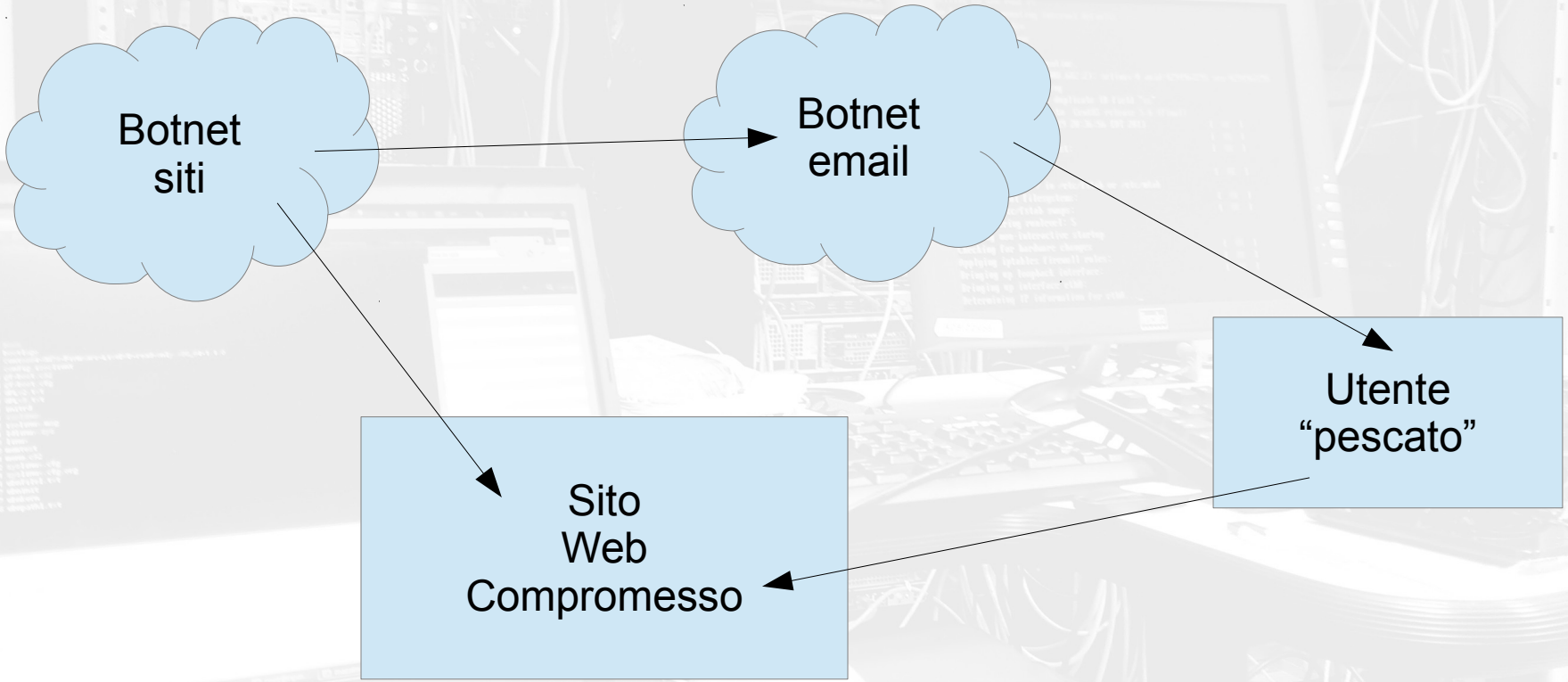
E poi ci sono i “cattivi”

- Sono la vera piaga odierna, ma di cosa si tratta?
- Phishing Attack / Brand Spoofing
- Cryptolocker
- Malware
- Etc...

Phishing

- Email con contenuto “verosimile” che rimandano a siti compromessi
- Servono a carpire informazioni molto riservate
- Conto corrente
- Carta di credito
- Ne esiste una versione per carpire id e password della posta elettronica...

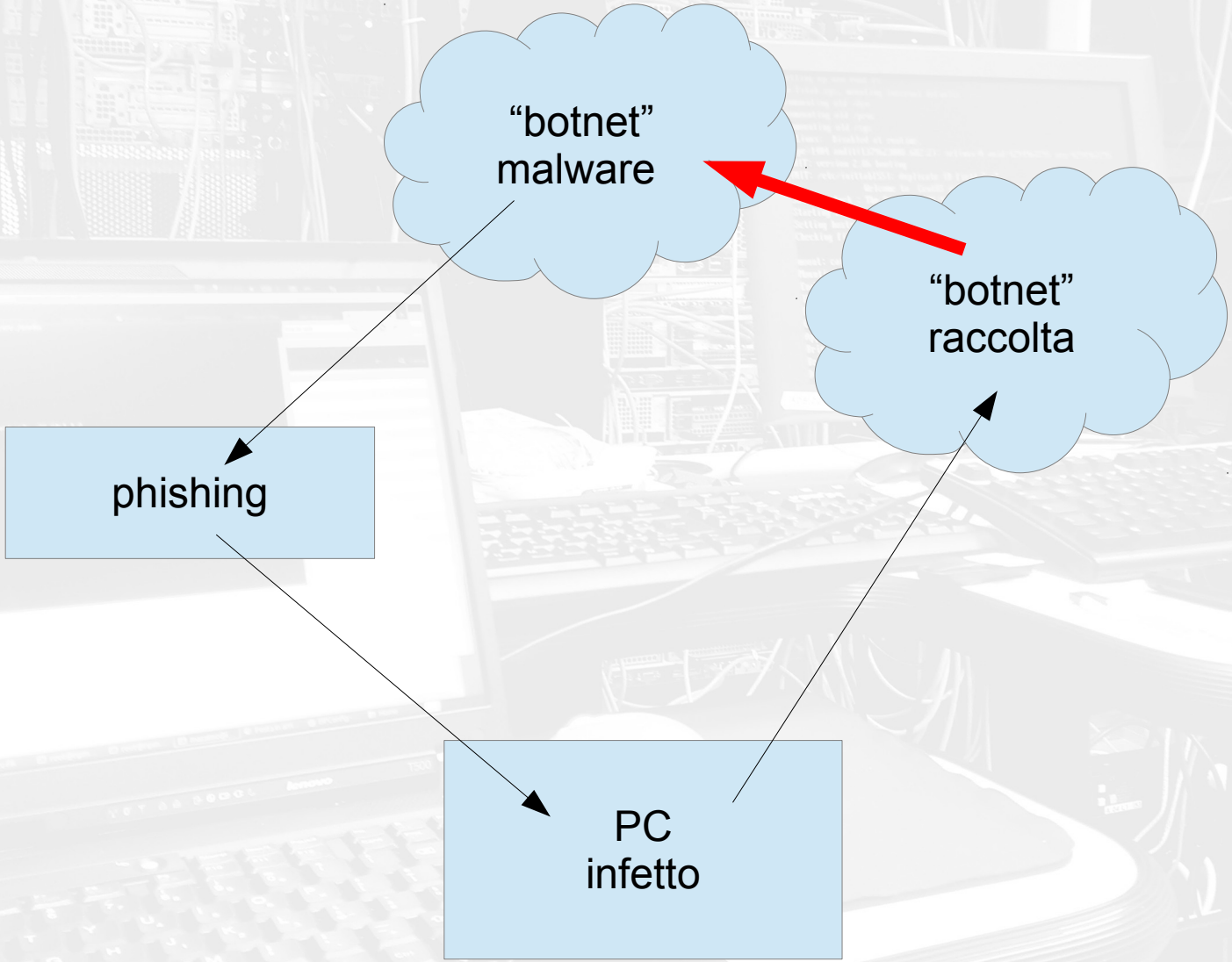
Come nasce il phishing?



Cryptolocker

- E' un software che si diffonde “principalmente” tramite la posta elettronica
- Si installa sulla macchina e usando degli strumenti standard “protegge” con la crittografia i dati
- Peccato che la password la invii a dei malviventi
- Riscatto!

Come funziona il cryptolocker



Brand Spoofing

- Colpisce i nomi “famosi” e serve soprattutto per carpire id e password
- Microsoft, Yahoo, Gmail, Ebay, Twitter etc...
- Alimenta il nuovo spam, quello basato sui social network
- Combattutissimo, ma é l'ombra occulta del successo dei social network stessi
- La profilazione é uno strumento potentissimo per dare piú efficacia allo Spam!

Malware

- Erroneamente pensato come fine a se stesso
- Sono software che vengono usati per carpire informazioni soprattutto in ambito aziendale
- Vengono utilizzati “anche” per alimentare lo spam stesso
- Per aggirare SPF DKIM e DMARC e il resto vanno utilizzati account di posta buoni
- La loro natura é piú subdola perché restano nascosti!

Lo Spam é “Statistica” ...

- Il funzionamento é quello della pubblicitá, ne fai molta, tantissima scegliendo un “target”* enorme, in base alla qualitá e alla quantitá avrai una certa percentuale di “redemption”*
- Il target é quindi casuale (in parte) quindi abbiamo una redemption casuale, ovviamente molto molto piccola in termini percentuali (tipo campagna pubblicitaria sbagliata)
- MA visto che lo spam tendenzialmente “non costa” qualsiasi risultato ottenuto rappresenta una vittoria (tipo campagna pubblicitaria molto proficua)

  * termini non a caso del marketing

… e si combatte con la “Statistica”!

- Per analizzare il traffico di posta ed i comportamenti sospetti dei server
- Per valutare la possibilitá che un messaggio sia spam
- Per valutare se un contenuto é pericoloso
- Per valutare la reputazione del mittente e del destinatario

Lotta Impari

- La lotta contro lo spam é sempre stata caratterizzata da una differenza sostanziale tra:
  - costo delle email (nullo)
  - ritorno economico (per quanto basso comunque rilevante)
- Se le email fossero a pagamento non esisterebbe il “fenomeno spam”

L'avvento dei cryptolocker

- Parte nel 2016 pesantemente
- La lotta diventa ancora piú impari, molti colpiti hanno pagato difatto sovvenzionando I criminali
- Denaro = migliori cryptolocker piú mirati e piú difficili da fermare
- Spesso vengono raccolti indirizzi email delle rubriche e anche messaggi “tipo” da utilizzare per successivi attacchi mirati
- Stiamo combattendo “con un coltello contro una mitragliatrice”

Come si combatte lo spam?

- Iniziamo dal protocollo SMTP
- Negli anni 80/90 sono stati eliminati e banditi I cosiddetti relay aperti (comuni prima), sono stati terreno fertile per la crescita del fenomeno
- E' solo un primo assaggio

Classificazione

- Ogni messaggio viene “classificato” e gli viene attribuito un valore di spamminess
- Normalmente da 0 a 50% non é spam (o lo é poco probabilmente)
- Da 50% a 80% lo é forse
- Da 80% a 100% (e piú) sicuramente é spam
- Ma queste soglie NON sono standard!

Falsi Positivi e Falsi Negativi

- Classificando I messaggi abbiamo due errori in genere:
  - I falsi positivi (cioé messaggi che vengono marcati come spam ma che non lo sono)
  - I falsi negativi (cioé messaggi che non vengono marcati come spam ma che in realtá lo sono)
- In pratica ogni volta che la classificazione si sposta sopra o sotto la soglia dello “spam” per errore incappiamo in uno di questi incidenti
- La bontá del sistema antispam restringe il numero di messaggi erroneamente classificati al minimo

Blocklist

- Si inizia dagli anni 90 a raccogliere gli ip delle botnet e degli open relay
- Si qualificano per qualitá e nasce il concetto di reputazione
- Se un ip appare in una blocklist si ha un buon motivo per considerare spam email che arriva da lí
- Il filtro a livello di blocklist agisce a livello di connessione TCP/IP, ed é responsabile del 90% circa del lavoro dei filtri antispam

Blocklist pro e contro

- Scaricano molto I filtri antispam
- E' necessario delegare ad entitá esterne (le blocklist normalmente sono pubbliche e/o a pagamento)
- Se per un errore (o per un problema tecnico) un ip finisce in blocklist va richiesto il delisting, ed alcuni si fanno pagare per farlo
- I grandi provider male organizzati finiscono spesso in blacklist (Tiscali, Tim, Outlook etc. etc.) e fornendo email gratis non hanno molti incentivi a migliorare questa cosa
- Ottimo motivo per non usare servizi “gratis”

SPF

- Sender Policy Framework
- Tecnica per impedire il recapito di email provenienti da un dominio provenienti da server non autorizzati
- Si basa sui DNS, nel dominio va aggiunto un record txt contenente le informazioni su SPF
- Esempio:

  "v=spf1 a mx ip4:193.33.98.0/23 a:pmx1.celta.it a:pmx2.celta.it a:pmx.celta.it ~all"

SPF pro e contro

- Non é ancora totalmente diffuso
- Viene utilizzato come “metro” per valutare la provenienza
- Basta usare un dominio senza SPF per scardinarne la forza
- Le implementazioni restrittive incidono sul funzionamento delle mailing-list

DKIM

- DomainKeys Identified Mail
- E' una tecnica che dovrebbe identificare ed evitare l'email spoofing
- I messaggi vengono firmati digitalmente dal server che li manda, se la firma non c'é o non é valida sicuramente il messaggio non arriva dal server giusto

DKIM pro e contro

- Scarsamente diffuso
- Interviene modificando I messaggi, rompe quindi I meccanismi di firma digitale sul messaggio intero
- Esistono superfici di attacco per fregare DKIM e quindi aggirare il meccanismo di valutazione che lo utilizza
- Se ben implementato é un ottimo strumento, ma solo per classificare in parte I messaggi
- Le implementazioni “troppo strette” finiscono per classificare come spam messaggi leciti
- Grana non da poco, é coperto da un Brevetto di Yahoo...

DMARC

- Domain-based Message Authentication, Reporting and Conformance
- DMARC é costruito partendo da DKIM e SPF, si basa su di essi ma non é obbligatorio che entrambe siano “ok”
- Classifica i messaggi partendo dal record “From:” ovvero il mittente
- Usa firme digitali per evitare la manomissione del mittente
- Introduce un meccanismo di feedback, la valutazione torna al mittente

DMARC pro e contro

- É poco diffuso
- Nel risultato di classificazione é ottimo, ma é applicabile in contesti limitati e con molti limiti
- Stessi limiti di SPF e DMARC
- Cattive implementazioni generano molti falsi positivi

Analisi per regole

- Servono dei database molto aggiornati e completi
- Aggiungono valutazione alle precedenti giá fatte
- Le regole agiscono sia su contenuto che header dei messaggi

Valutazione Statistica

- Se é possibile identificare messaggi buoni (e soprattutto cattivi) si puó insegnare al filtro antispam a riconoscere le mail
- Essendo statistica va da se, puó sbagliare

Controllo allegati

- Gli antivirus si sono dimostrati inefficaci contro le minacce moderne, cambiano troppo e troppo frequentemente
- Si preferisce agire a livello piú basso tipo “comportamento sospetto”
- Per policy (e sanitá mentale) non andrebbero mai spediti file modificabili
- Oramai eseguibili (.exe .com .vbs .js etc.) e tanti altri file non passano piú i filtri
- La crittografia e le password sono la nuova frontiera

Sopravvivenza

- Usare sempre smtp, pop3, imap con crittografia per evitare il password sniffing
- Cambiare le password il piú spesso possibile e non usare password identiche ovunque
- Se prendete un cryptolocker le password vanno cambiate tutte, si aspetta una settimana, e poi si ricambiano tutte

MITM via mail

- Man In The Middle
- E' un attacco “indiretto”, finalizzato ad interporsi nelle comunicazioni email.
- Una buona base sono credenziali email sottratte, in questo modo é possible (con imap ad esempio) manipolare la mail inviata e ricevuta per adattarla ai propri scopi
- Soprattutto in ambito aziendale é un danno grandissimo

Se siete vittime

- Phishing: cambiate le password subito, bloccate il conto, la carta tutto, oramai é facile e veloce
- Cryptolocker: se avete aperto un cryptolocker e ne siete certi STACCATE LA SPINA, spegnete i server, tutto e affidatevi ad un professionista
- Anche per obblighi relativi al GDPR dovete sempre sporgere denuncia alla Polizia Postale (qua a Torino andate in Corso Tazzoli), sono competenti e oltre ad aiutarvi servono per evitare il peggio


DOMANDE?

per contattarmi:

maxnuv@linux.it