SOCIAL ENGINEERING

- UTILIZZATO IN AMBITO PRETTAMENTE INFORMATICO, E' QUELL'INSIEME DI TECNICHE UTILIZZATE AL FINE DI CARPIRE INFORMAZIONI UTILI E NECESSARIE PER PERPETRARE AZIONI FRAUDOLENTE.

- SFRUTTA TOTALMENTE IL FATTORE UMANO: ED E' PER QUESTO CHE ANCORA OGGI E' UNO DEGLI STRUMENTI PIU' UTILIZZATI DAI CRIMINALI INFORMATICI.

TECNICHE UTILIZZATE

- **PHISHING** - EMAIL FASULLE SU LARGA SCALA
- **WATER HOLING** - LEVA SU SITI WEB CONOSCIUTI
- **BAITING** - CAVALLO DI TROIA FISICO

LUOGHI COMUNI DA SFATARE

1. **I CRIMINALI INFORMATICI PREFERISCONO GLI ATTACCHI LAMPO**
2. **SERVIZI LEGITTIMI COME QUELLI FORNITI DA GOOGLE E MICROSOFT POSSONO ESSERE UTILIZZATI IN MODO SICURO**
3. **I CRIMINALI INFORMATICI UTILIZZANO SOLO LA MAIL**
4. **LE CONVERSAZIONI INTERNE ALL'AZIENDA SONO SICURE**
5. **I CRIMINALI INFORMATICI UTILIZZANO SOLO CONTENUTI STANDARDIZZATI A CARATTERE PROFESSIONALE**

METODOLOGIE DI DIFFUSIONE

1. **QR CODE**
2. **LE NOTIFICHE**
3. **LE FINTE COLLABORAZIONI**
4. **L'INTELLIGENZA ARTIFICIALE**
5. **INVIO DI SMS (SMISHING)**

COS’E’ IL PHISHING

- PARTICOLARE TIPOLOGIA DI TRUFFA REALIZZATA ATTRAVERSO L' INGANNO DEGLI UTENTI
- SI CONCRETIZZA PRINCIPALMENTE ATTRAVERSO MESSAGGI DI POSTA ELETTRONICA INGANNEVOLI.

METODOLOGIE DI PREVENZIONE

- MAI FIDARSI DEL MITTENTE. PUO' ESSERE FACILMENTE CONTRAFFATTO. E' NECESSARIO VERIFICARE L'INTESTAZIONE DEL MESSAGGIO
- L'ESTENSIONE DI UN FILE ALLEGATO,PUO' ESSERE MASCHERATA. E' NECESSARIO VERIFICARE CON ESATTEZZA L'ESTENSIONE DEI UN FILE
- I LINK NON SEMPRE CORRISPONDONO ALLA REALTA'. CONTROLLARE L'INTERO INDIRIZZO INDICATO NEL COLLEGAMENTO

LE 10 REGOLE ANTI PHISHING

- NON FIDARTI MAI DEL MITTENTE
- NOTA SE CI SONO ERRORI GRAMMATICALI NEL TESTO
- CONTROLLA LA FORMA DEL SALUTO
- CONTROLLA SEMPRE LA FIRMA DEL MESSAGGIO
- DIFFIDA DAI TONI ALLARMISTICI
- GUARDARE MA NON CLICCARE

LE 10 REGOLE ANTI PHISHING

- GUARDARE MA NON CLICCARE
- NON APRIRE MAI GLI ALLEGATI
- VERIFICA LE INTESTAZIONI
- NON SI DANNO MAI DATI PERSONALI
- E SE UTTO SEMBRA APPOSTO… NON FIDARTI

VIRUS

Un virus informatico è una serie di istruzioni scritte da un programmatore ed eseguibili da un computer, il quale ha le seguenti caratteristiche:

- È stato scritto per "inglobarsi" e cioè confondersi alle istruzioni di altri programmi modificandoli.
- Chi l‘ha scritto ha previsto la possibilità che il virus sia in grado di copiare le istruzioni che lo compongono in altri programmi .

LE TIPOLOGIE DI VIRUS

Uno **spyware** è un software che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto.

I **macro virus** sono generalmente script incorporati all'interno di particolari documenti (come ad esempio Word, Excel...).

Un **worm** (letteralmente "verme") è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri file eseguibili per diffondersi.

I **Trojan** sono dei virus che non fanno alcun danno ma permettono, al loro creatore di accedere al computer e di prenderne il pieno possesso. Sono legati al download di un file

Il malware (abbreviazione di *"malicious software"* – software malevolo) è un file o un codice, generalmente distribuito su una rete, che infetta, esplora, ruba o conduce praticamente qualsiasi comportamento desiderato da un utente malintenzionato.

MALWARE

Il malware (abbreviazione di *“malicious software”* – software malevolo) è un file o un codice che infetta, esplora, ruba o conduce praticamente qualsiasi comportamento desiderato da un utente malintenzionato.
Sebbene sia vario per tipologia e capacità, un malware di solito ha uno dei seguenti **obiettivi**:

- **Fornire il controllo remoto a un utente malintenzionato per utilizzare una macchina che è stata infettata.**
- **Inviare spam dalla macchina infetta a obiettivi ignari.**
- **Indagare sulla rete locale dell’utente infetto.**
- **Rubare dati sensibili**.

MALWARE – COME ACCORGERSI

- Il tuo computer è rallentato e impiega più tempo per avviarsi
- Inspiegabili blocchi o arresti anomali (*"Blue Screen of Death"* (BSOD)
- Annunci pop-up o avvisi di sicurezza sospetti
- Richieste di riscatto
- Tutto sembra normale (condizione che potrebbe valere per uno spyware)

TROJAN HORSE

Un **Trojan** è un malware che si traveste da codice o software attendibili. Una volta scaricato da utenti ignari, il Trojan può assumere il controllo dei sistemi delle vittime per scopi dannosi. I trojan possono nascondersi all'interno di giochi, app o persino patch software, oppure possono essere incorporati in allegati inclusi in e-mail di phishing.

SPYWARE

Lo **spyware** raccoglie informazioni sulle attività degli utenti a loro insaputa o senza il loro consenso. Questo può includere password, pin, informazioni di pagamento e messaggi non strutturati.

L'uso dello spyware non si limita al browser desktop: può funzionare anche all'interno di un' app critica o su un telefono cellulare.

Anche se i dati rubati non sono importanti, **gli effetti dello spyware spesso si ripercuotono sull'intera organizzazione** poiché le prestazioni vengono ridotte e la produttività viene erosa.

KEYLOGGER

Un **keylogger** è un tipo di spyware che monitora l'attività dell'utente. I keylogger hanno anche usi legittimi: le aziende possono usarli per monitorare l'attività dei dipendenti e le famiglie possono usarli per tenere traccia dei comportamenti online dei bambini.

Tuttavia, se installati per scopi dannosi, i keylogger possono essere **utilizzati per rubare dati** di password, informazioni bancarie e altre informazioni sensibili. I keylogger possono essere inseriti in un sistema tramite phishing, social engineering o download dannosi.

WORM

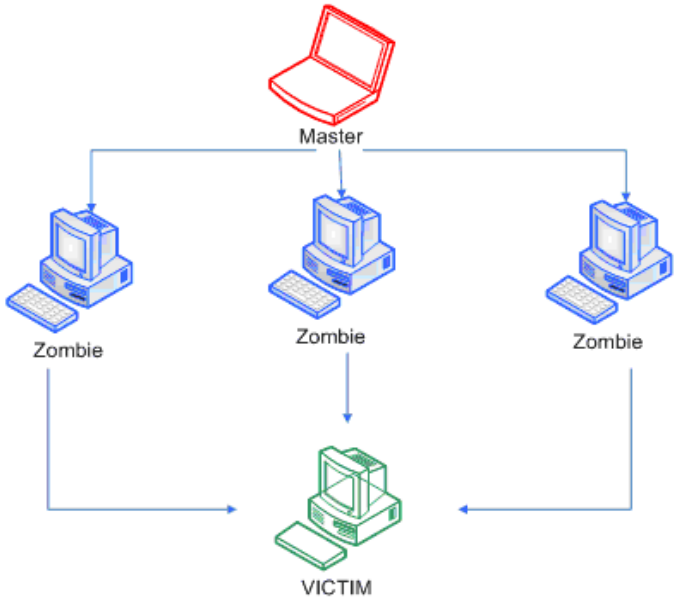
I **worm** prendono di mira le vulnerabilità dei sistemi operativi per installarsi all'interno delle reti. Possono accedervi in diversi modi: tramite backdoor integrate nel software, tramite vulnerabilità software non intenzionali o tramite unità flash. Una volta installati, i worm possono essere utilizzati da attori malintenzionati per lanciare attacchi DDoS, rubare dati sensibili o condurre attacchi ransomware

RANSOMWARE

Il **ransomware** è un software che utilizza la crittografia per disabilitare l'accesso di un bersaglio ai suoi dati fino a quando non viene pagato un riscatto. L'organizzazione vittima è resa parzialmente o totalmente incapace di operare fino a quando non effettua il pagamento, ma non vi è alcuna garanzia che ciò si tradurrà nella chiave di decrittazione necessaria o che la chiave di decrittazione fornita funzionerà correttamente.

DENIAL OF SERVICE

- Nella sicurezza informatica **DDoS**, è la sigla di **Denial of Service**, letteralmente *negazione del servizio*.
- Si tratta di un malfunzionamento dovuto ad un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio online, ad esempio un sito web, fino a renderlo non più in grado di erogare il servizio.



I PROTOCOLLI

Per ovviare alla vulnerabilità dei protocolli utilizzati per la gestione della posta elettronica, sono stati introdotti servizi che garantiscono:

- L'autenticazione del messaggio di posta elettronica definendo i nodi autorizzati a spedire messaggi
- L'autenticità del messaggio di posta elettronica, garantendo la non violazione dei contenuti

LE BUONE RAGIONI DI UN BACKUP DEI DATI

- Backup dei dati in informatica è **sinonimo di continuità operativa**. Compiere questa operazione, infatti, significa fare un duplicato e quindi creare una **copia di sicurezza di informazioni e file**. Per quanto noioso, questo è l'unico modo che permette agli utenti di proteggere i dati.

COME FARE UN BACKUP DEI DATI

- Come si fa il back up? Vero è che oggi **la maggior parte delle grandi aziende ha adottato soluzioni allo stato dell'arte**. Il mondo enterprise può contare su SAN di fascia alta, alimentate dai miglior array di dischi e sistemi di backup di dati multilivello, integrate da piani di DR. Le grandi aziende hanno anche le risorse per comprare maggiore spazio quando ne hanno bisogno. Oppure possono decidere di potenziare l'uso del back up dei dati in cloud.

E SE NON ESEGUO IL BACKUP DEI DATI

- Non eseguire il backup dei tuoi dati è un grosso problema. Senza il backup potresti non avere più accesso a informazioni o file importanti per te o per la tua azienda.
- Si pensi alla **eventualità di un attacco ransomware**. In tali occasioni gli hacker rendono inutilizzabili i dati sino al pagamento di un riscatto. Avere il backup dei dati significa non esporsi al rischio di ricatti ed essere comunque operativi

COME CREARE UNA BUONA PASSWORD

- RICORDA - PENSA A QUALCOSA A TE CARO
- DESCRIVI - PENSA A QUELLO CHE PROVI
- COMPRIMI - SINTETIZZA CON LE SOLE INIZIALI
- AGGIUNGI - NUMERI E/O CARATTERI SPECIALI
- SOSTITUISCI - CAMBIA ALCUNE LETTERE

COME CREARE UNA BUONA PASSWORD

- RICORDA - CONCERTO POLICE 2007
- DESCRIVI - IL CONCERTO PIU' BELLO DELLA MIA VITA
- COMPRIMI - ICPBDMV
- AGGIUNGI - ICPBDMV07!
- SOSTITUISCI - 1CP8DMV07!

L’ANTIVIRUS

- Un antivirus è un programma che blocca l'esecuzione o la memorizzazione nel sistema del malware.
- L'antivirus viene immediatamente avviato dal sistema operativo e viene invocato prima che un programma venga eseguito e prima che un file venga memorizzato nel sistema (download da Internet, copia da chiavetta, ecc.).
- L'antivirus verifica se il programma in procinto di essere eseguito o il file in corso di memorizzazione è presente nel catalogo delle definizioni del malware. Se è così l'antivirus blocca l'esecuzione del programma o la memorizzazione del file.
- Il catalogo delle definizioni deve essere costantemente aggiornato per consentire all’antivirus di essere efficace

UNA SOLUZIONE

virustotal

SHA256: 6cfe3e7e1a680fecf200c4e63a9239b3a1c52c31a8d50204828ccf1bbcab7663

File name: 20170318_srv01_update.txt

Detection ratio: 0 / 56

Analysis date: 2017-04-08 16:58:57 UTC (0 minutes ago)

Analysis | Additional information | Comments | Votes

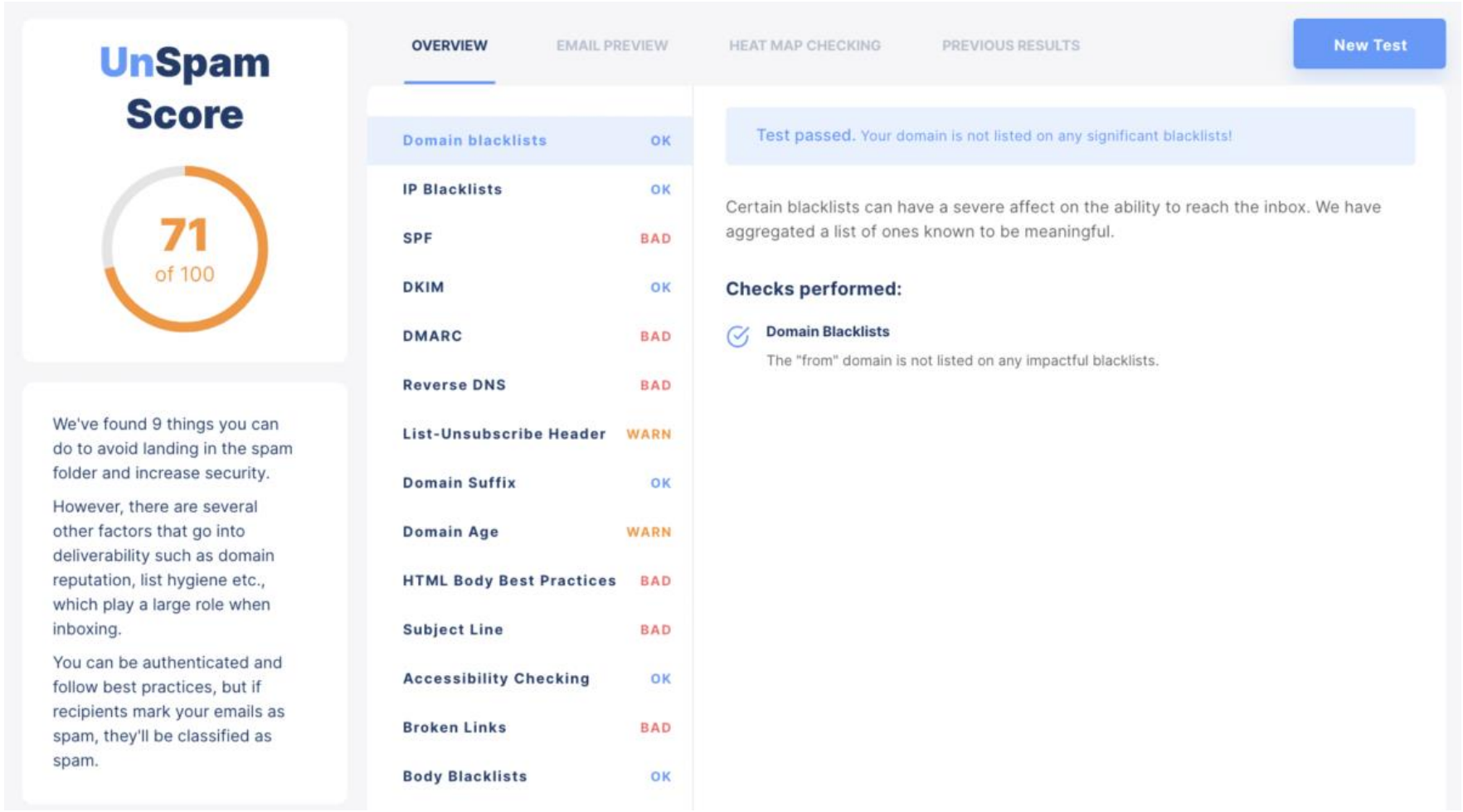
Antivirus	Result	Update
Ad-Aware	✓	20170408
AegisLab	✓	20170408
AhnLab-V3	✓	20170408
Alibaba		20170407
ALYac	✓	20170408
Antiy-AVL	✓	20170408
Baidu	✓	20170406
BitDefender	✓	20170408

itcore GROUP

IL PROBLEMA DELLO SPAM

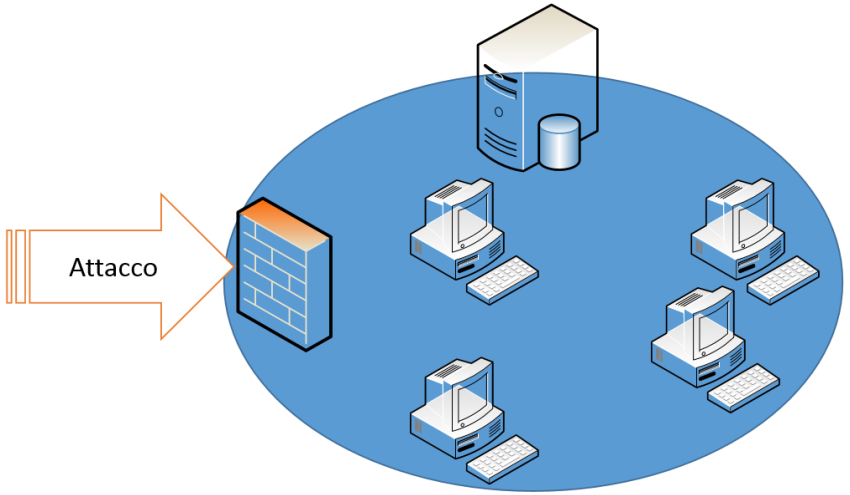
- Ma sei sicuro che le tue email arrivino tutte correttamente ai destinatari?
- **Cosa ti garantisce che le tue email non vanno finire in spam**?
- Come puoi controllare la reputazione del tuo dominio se sei finito in qualche blacklist?
- Molto spesso, infatti, accade che **una email non venga consegnata come dovrebbe**, e che venga contrassegnata dai server di posta, come SPAM, andando a finire direttamente nella cartella spam o venendo addirittura bloccata a livello di server.

UNA SOLUZIONE



PROTEZIONE PERIMETRALE

Il firewall è un apparato di rete hardware o un software che filtra i pacchetti entranti ed uscenti, da e verso una rete o un computer, secondo regole prestabilite. Configurando opportunamente le regole è possibile bloccare i pacchetti non desiderati cercando così di proteggere la rete o il singolo computer da attacchi diretti da parte di pirati informatici o da software che cercano di violare il sistema.



COME DIFENDERSI DA UN ATTACCO DI PHISING

- Alla base della difesa rimane sempre l'attenzione agli elementi che compongono una mail (mittente, testo, allegati, link), un sito web (controllo dell'url), messaggeria istantanea (mittente, attendibilità del fornitore di servizi)
- Cercare informazioni legate alla cyber reputation del mittente
- Utilizzare dei sistemi di protezione come firewall (hardware e/o software) antivirus, antispam
- Utilizzare password robuste e cambiarle con frequenza
- Non divulgare mail informazioni personali
- Restare «formati» sull'argomento