L'ANELLO DEBOLE

L'utente e la sua collocazione nel network

whiteready
we take care of your net

L'ANELLO DEBOLE

Nella quotidiana operatività degli uffici (PMI, studi professionali, consulenti) la quasi totalità dei rischi proviene da un numero limitato di vettori.

- La posta
- Il web
- Altro

L'anello più debole delle struttura difensiva è l'utente, la cui collaborazione (attiva o passiva) è quasi sempre richiesta.

I VETTORI DI ATTACCO

- Posta
  E’ certamente il canale più facilmente utilizzabile, attraverso cui è possibile introdurre codice malizioso **all’interno** delle reti e delle strutture private.

- Web
  Fishing e social engineering
  Crypto mining
  Malware

- Altro
  Keylogger
  Accessi non autorizzati
  Devices insicuri

whiteready
we take care of your net

SCOPI DEGLI ATTACCHI

- La maggior parte degli attacchi portati ai device degli utenti non ha come obiettivo l'utente stesso.
- Escludendo il fishing e le truffe informatiche in genere, lo scopo è quello di accedere a risorse (macchine o servizi) utilizzate dalla vittima.
  - Posta: utilizzare gli account utente per inviare spam
  - Utilizzare gli accessi al network aziendale per diffondere ransomware
  - Acquisire informazioni di sistema
  - Acquisire il controllo del device per usarlo all'interno di botnet e portare attacchi a sistemi esterni

LO SPAM COME MOTORE GENERALE DI ATTACCO

Lo spam è il primo strumento per qualsiasi tipo di attacco monetizzabile

Qualsiasi tipo di attacco, per essere significativo e redditizio, ha la necessità di coinvolgere grandi quantità di device.

Lo spam è lo strumento più efficace per fare social engineering e/o per diffondere direttamente malware, assumere il controllo dei device e utilizzarli come moltiplicatori, penetrare nei network locali.

L'attività più *basic* dei cybercriminali è acquisire il controllo di caselle di posta e utilizzarle (anche per breve tempo) per inviare spam da sorgenti *trusted*.

IL CRYPTO MINING

Negli ultimi mesi sta emergendo un nuovo utilizzo monetizzabile dei device utenti: il Browser-Based Cryptocurrency Mining.

L'attività di mining delle cryptovalute richiede enormi capacità di calcolo, che la rendono in perdita se a carico proprio. Nascono quindi alcuni malware che trasferiscono sulla macchina utente il lavoro di mining. Questo avviene sia tramite virus installati sia tramite pagine web compromesse.

LE BOTNET

- Diffusione: attraverso lo spam, tramite botnet

➤ Nel primo trimestre del 2017 la quota di spam nel traffico di posta elettronica si è attestata al 55,9%. Nei mesi precedenti era intorno all'86%.

➤ La maggior parte di questo spam è stato generato dalla botnet Necurs, la più estesa del mondo.

➤ Gli scopi più comuni ed evidenti erano la distribuzione di ransomware e di un malware riconducibile alla famiglia Pony/FarelIT, sintesi di quasi tutti i malware in circolazione.

whiteready
we take care of your net

PONY/FARELIT: COSA PUÒ FARE

- Eseguire il furto degli username e delle password – memorizzati sul browser dell'utente – utilizzati per accedere ai servizi web;
- Carpire gli indirizzi URL in cui tali credenziali sono state introdotte;
- Impadronirsi dei dati necessari per eseguire le procedure di autenticazione nell'ambito dei server FTP, dei file manager, dei client di posta elettronica, delle applicazioni di sincronizzazione.

I programmi Trojan riconducibili alla famiglia Pony/FarelIT, temibili stealer di informazioni, vengono inoltre utilizzati per compiere il furto dei wallet (portafogli virtuali) contenenti criptovaluta.

L'UTENTE

All'interno delle dinamiche criminali, l'utente quasi mai ha consapevolezza alcuna del suo ruolo.

- Non riceve danni diretti (o almeno non ne ha evidenza)
- Non è l'obiettivo vero dell'attacco
- Spesso collabora attivamente con il malware
- Può scaricare le sue responsabilità su terzi
- Non ha sufficienti competenza e consapevolezza

In sostanza, è il vettore ideale di infezioni di varia natura

whiteready
we take care of your net

IL RUOLO DEI SISTEMISTI

Lungi dal poter **garantire** un ambiente privo di rischi, il sistemista può creare un sistema di controlli, di procedure, di permessi etc per ridurre i possibili danni.

Può agire a diversi livelli e in diversi ambiti.

- Gestione dei servizi esterni
- Gestione della rete interna
- Gestione dei singoli device
- Formazione e responsabilizzazione utente
- Monitoraggio ad ampio spettro

whiteready
we take care of your net

LA POSTA, LATO SISTEMISTA

Sui server di posta si può (e si deve) adottare qualsiasi misura, lecita e affidabile, utile a innalzare il livello generale di sicurezza degli utenti.

Questo si traduce principalmente in

- Proteggere al meglio il server e le infrastrutture collegate
- Ridurre lo spam che arriva all'utente
- Analizzare la posta rimanente per espungere possibili minacce
- Imporre policy di sicurezza agli utenti
- Sensibilizzare gli utenti sull'uso fraudolento degli account

LO SPAM, IL VETTORE/UNTORE

Lo spam è il pericolo maggiore che minaccia tutto l'IT.

Di tutte le misure che si possono intraprendere per mettere in sicurezza la LAN, la più irrinunciabile è ridurre al minimo lo spam.

Al secondo posto la formazione degli utenti: nessun sistema automatico può bloccare tutte le minacce, in particolare quelle di nuova generazione. Se ne può ridurre la quantità e mitigare l'impatto ma non se ne può escludere completamente il pericolo.

GRAZIE!

HTTPS://WHITEREADY.COM