LOOKING FOR CHANGE

Nom: Pol Fuster
Victor Joven

Henry Funes

Escolliu un malware:

- Classifiqueu-lo.
- Determineu la gravetat i l'impacte sobre un sistema.
- Establiu mesures de prevenció. Identifiqueu mecanismes de protecció del sistema contra malware.
- Dissenyeu un pla d'acció per solucionar l'atac en cas que no s'hagi pogut prevenir.

Llista de malware

- **Virus:** Programes, que a l'executar-se, infecten parts de l'ordinador, ja siguin processos, o altres programes grans, alterant el seu funcionament de diverses maneres, en els pitjors casos, danyant el sistema.

- **Spyware:** Aquest programari, s'inicia amb el nostre equip i recull tota la informació possible del nostre ordinador i la transmet a un altre equip. Afecta la nostra privacitat, al rendiment del nostre equip i als recursos de xarxa.

- **Rootkit:** Aquest conjunt de programes està dissenyat per modificar el sistema operatiu amb l'objectiu de crear una porta del darrere que pugui ser utilitzada pels atacants per accedir a sistema remotament sense ser detectats. Les vulnerabilitats de programari són aprofitades per aquest malware per modificar arxius de sistema i així generar aquesta entrada del darrere.

- **Cucs:** Tenen la capacitat de copiar-se a si mateix propagar-se a altres equips en la mateixa xarxa, afectant ràpidament a un gran nombre de dispositius, aquests poden ser una gran amenaça en grans estructures i afectant en gran mesura a el tràfic de la nostra xarxa, creant una infinitat de comunicacions entre dispositius que col·lapsin la xarxa.

- **Ransomware:** Aquest malware està creat per a restringir o bloquejar l'accés a certes parts o arxius d'un sistema infectat amb l'objectiu de demanar un rescat per això. Generalment aquest tipus de programa treballa encriptant les dades amb una clau desconeguda per a l'usuari, algunes versions també aprofiten vulnerabilitats de sistema per bloquejar-lo.

- **Phishing:** És un mètode per infectar-nos amb qualsevol tipus de programari, aquest mètode es basa en enviar informació per correu, fent-se passar per entitats conegudes i fent que la víctima entri al URL maliciosa.

Com hem escollit

Ransomware: Aquest malware està creat per a restringir o bloquejar l'accés a certes parts o arxius d'un sistema infectat amb l'objectiu de demanar un rescat per això. Generalment aquest tipus de programa treballa encriptant les dades amb una clau desconeguda per a l'usuari, algunes versions també aprofiten vulnerabilitats de sistema per bloquejar-lo.

Hem escollit aquest Malware ja que considerem que és un dels més perillosos i volem saber com prevenir aquests atacs. Les pautes a seguir per evitar-lo són:

- Mantenir les aplicacions i el Sistema Operatius ben actualitzats.
- Instal·lar un antivirus amb seguretat extrema(de pagament).
- Instal·lar el tallafocs més complert que trobem per poder protegir els nostres equips de totes les amenaçes possibles.
- Desgarregar i instalar programari Anti Ransom per bloquejar l'accés a arxius cifrats d'un ransomware.
- Aplicar un filtre antispam a tots els correus elèctrònics de l'empresa.
- No utilitzar comptes d'Administrador per a tasques comuns, només en cas de manipulació del sistema.
- Realitzar còpies de seguretat diàriament.

Gravetat i l'impacte sobre un sistema

L'atac a un usuari amb permisos d'administrador i amb control total dels usuaris assignats al domini és més greu que si ataquen a un usuari sense permisos.

- Pot agafar molta informació valiosa, sobretot econòmicament parlant.
- Pots perdre tots els arxius dels sistemes afectats.
- Pots perdre informació important si t'ataquen un servidor si no tens còpia de seguretat.

Dissenyeu un pla d'acció per solucionar l'atac

- La recomanació habitual és no pagar el rescat, ja que ningú ens assegura que podem recuperar els arxius infectats, a més pot ser que demanin encara més diners després de que es realitzi el primer pagament.
- Ja que tenim còpies de seguretat podríem intentar restablir-les completament a tots els sistemes afectats.
- Realitzar un clonat diari dels discs durs de cada ordinador per prevenir aquest tipus d'atacs.
- Instal·larem a tots els equips un programa anomenat Crypto-Sheriff que serveix per identificar quina variant de malware està sofrint el nostre sistema.

webgrafia

- https://rincondelatecnologia.com/tipos-de-malware/
- https://concepto.de/firewall/
- https://www.empresarius.com/2017/06/28/las-consecuencias-del-ataque-masivo-ransomware/