

17.- Seguretat

Javier FRANCÉS FALIP
David SÁNCHEZ MULERO

Taula de continguts

Taula de continguts	1
Enunciat	2
Introducció a la seguretat informàtica	2
Què és la ciberseguretat?	2
Perquè és important?	3
La seguretat i els CPD's.	4
Com són els atacs?	6
Modus operandi	6
Ciberamenaces més comuns	7
Equips de seguretat	11
Red team (Atac)	12
Eines de red team	14
Blue team (Defensa)	16
Eines de blue team	17
Casos pràctics	21
Objectius dels hackers	21
Cas 1. Adif	22
Cas 2. FireEye	23
Cas 3. SolarWinds	25
Cas 4. Microsoft Exchange	26
Bibliografia	27

Enunciat

En els últims mesos ha hagut molts atacs a companyies d'assegurances (es sap bastant de MAPFRE, però també Allianz, Caser i Pelayo) via ramsonware. La seguretat és un dels temes més importants en un CPD. Analitzeu els atacs rebuts (el que pugueu esbrinar i estudieu quines eines es poden fer servir com a protecció, com per exemple OSSIM (<https://www.alienvault.com/products/ossim>) un software open source per seguretat, un dels més utilitzats al món.

Introducció a la seguretat informàtica

Durant els darrers anys el món s'ha anat desenvolupant cada cop més en l'àmbit digital: les empreses cada cop més busquen digitalitzar els seus serveis i no només en aspectes laborals sinó que també en aspectes personals, tota la gent avui dia porta un smartphone, molta d'aquesta gent té totes les seves dades en aquests aparells. Molta d'aquesta informació és sensible o privada i d'aquí va sorgir la necessitat de protegir aquestes dades de possibles atacs o filtracions.

Què és la ciberseguretat?

El concepte de ciberseguretat concepte va néixer amb la necessitat de les companyies de protegir els seus sistemes informàtics d'atacs maliciós que puguin comprometre el seu correcte funcionament i fer un ús indegit de la informació obtinguda en ells, buscant generalment un benefici econòmic.

El Centre Criptològic Nacional d'Espanya denomina ciberseguretat al conjunt d'actuacions orientades a assegurar, en la mesura del possible, les xarxes i sistemes que constitueixen el ciberespai: detectant i confrontant-se a intrusions; detectant, reaccionant i recuperant-se d'incidents; preservant la confidencialitat, disponibilitat i integritat de la informació.

Dins de la ciberseguretat tenim persones amb molt coneixement sobre xarxes i sistemes informàtics a les que denominem "hackers". Hacker a priori ens ve al cap algú amb fins malèfics i il·legals però no és del tot correcte. A continuació expliquem els tres principals grups de hackers que hi ha.



Figura 1. Tipus de hackers.

Comencem amb els black hat. Aquests són el que tothom entén com dolents, utilitzen el seu coneixement per fer actes delictius, crear i distribuir malware, robar credencials, informació, destruir dades. Busquen principalment el benefici personal i fins i tot busquen malícia per l'emoció del ciberdelicte.

Per un altre costat estarien els white hat, aquests són els que utilitzen el seu coneixement per fer el bé, també se'ls coneix com hackers ètics. Aquests solen ser empleats, de l'equip informàtic de l'empresa o d'una empresa externa dedicada a la seguretat.

Els white hat utilitzen les mateixes eines que utilitzen els black hat, l'única diferència està en que els white hat tenen el permís del propietari del sistema per fer penetracions i buscar vulnerabilitats, el que fa que el procés sigui totalment legal.

De moment hem vist el dos extrems, ens queda un punt intermig, al que anomenem grey hat.

Diem que els grey hat son el punt intermig perquè realment estan al mig del dos extrems, fan accions tant de white hat com de black hat. Aquests hackers busquen vulnerabilitats en un sistema sense el permís del propietari i un cop han trobat una vulnerabilitat ho comuniquen al seu propietari a canvi d'una petita tarifa o un contracte de treball per solucionar el problema. Si el propietari no compleix, el grey hat publica la vulnerabilitat a internet perquè altres ho puguin explotar. Els grey hat no solen explotar les vulnerabilitats.

Perquè és important?

La ciberseguretat és important, millor encara, molt important i cada cop més. És important perquè a internet hi ha moltíssimes dades/informació, d'empreses, personals com targetes bancàries, íntimes... Els cibercriminals son conscients d'això i volen tota aquesta informació per el seu propi benefici o només per enfonsar a tal empresa o persona.

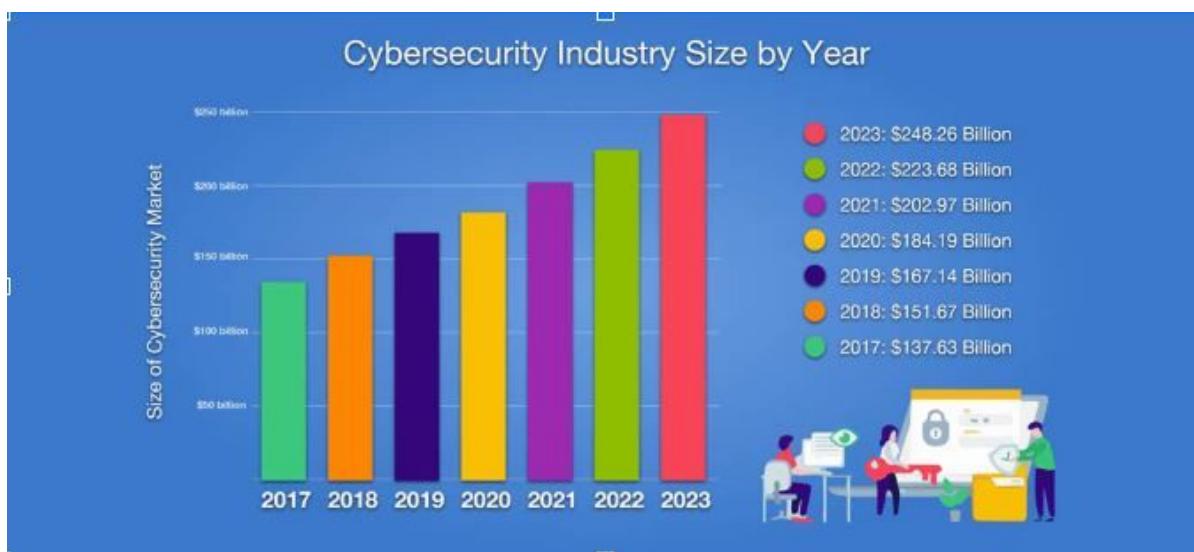


Figura 2. Gràfic de la mida de la ciberseguretat i possible previsió.

Cada any es destinen més diners a la ciberseguretat, això és degut a que cada cop més les empreses es donen compte de la importància de protegir aquestes dades, i de fer-ho adequadament seguint lleis com la Llei orgànica.

La importància de la ciberseguretat no només recau en les empreses, també en el usuaris quotidians d'internet que haurien d'estar conscienciatos. Per això es recomana seguir unes bones pràctiques i algunes d'aquestes serien:

- Utilitzar contrasenyes robustes
- Realitzar les compres online en webs de confiança i que tinguin certificat digital vàlid.
- No reenviar segons quins missatges en cadena.
- Ser cuidadós amb el que es publica a internet

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^3)
m – Million (1,000,000 or 10^6)
bn – Billion (1,000,000,000 or 10^9)
tn – Trillion (1,000,000,000,000 or 10^{12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{18})

Figura 3. Temps que triga en desxifrar una contrasenya segons la seva composició.

La seguretat i els CPD's.

La necessitat de protegir els CPD es la mateixa que es parla abans, els CPD son grans magatzems de dades.

En els CPD's la seguretat no només és a nivell d'informàtica sinó que també s'ha d'implementar una seguretat física. En aquesta seguretat física podem trobar-hi diferents camps.

El primer seria controlar l'accés al CPD, acompanyar a la gent externa i posar càmeres de videovigilància. El CPD és millor mentre més ocult sigui, per tant les parets han de ser d'algún material opac i ocultar en tot el que sigui possible la seva ubicació.

Hem de tindre mesures contra incendis. El cablejat ha d'estar etiquetat el màxim possible i els cables millor si son apantallats.

Hem de disposar de sistemes d'alimentació ininterromputs i mantenir una bona climatització a l'ambient del CPD.

Totes aquestes mesures son una bona praxis per mantenir la seguretat a nivell físic.

A nivell informàtic hem d'assegurar que el sistema operatiu sigui segur. Les contrasenyes dels administradors han de ser segures, hem de posar llistes d'accés (ACL) per restringir el tràfic, s'ha de restringir els privilegis i minimitzar l'ús d'usuaris com root. Hem de desactivar els serveis que siguin necessaris per tal de tindre menys possibles punts de fallida. S'ha de gestionar bé els recursos que utilitza cada procés perquè en cap moment doni una denegació de servei. Hem d'utilitzar software de seguretat com poden ser els antivirus o els HIDS (host intrusion detection system). Per últim podem fer configuracions segures, hi ha entitats que donen guia per fer aquestes configuracions, un exemple seria NIST (National Institute of Standards and Technology).

No només hem de protegir el sistema operatiu sinó que també les aplicacions. Les aplicacions que es connecten al CPD solen ser client/servidor, model en el qual un o més clients es connecten al servidor per escriure, llegir o fer alguna operació. Exemples d'aplicacions serien, correu electrònic, aplicacions de gestió de base de dades o aplicacions web.

Les mesures que hem de tindre en compte son molt semblants a les del sistema operatiu, s'ha d'identificar i autenticar a cada usuari correctament, això permet també saber qui és responsable de cada acció realitzada, s'ha de monitoritzar cada acció incloent-li data, hora i autor. Igual que al sistemes operatius s'ha de deshabilitar les opcions que siguin innecessàries.

Tant en aplicacions com en sistemes operatius s'ha d'anar fent auditories i test d'intrusions per tal de verificar la seguretat.

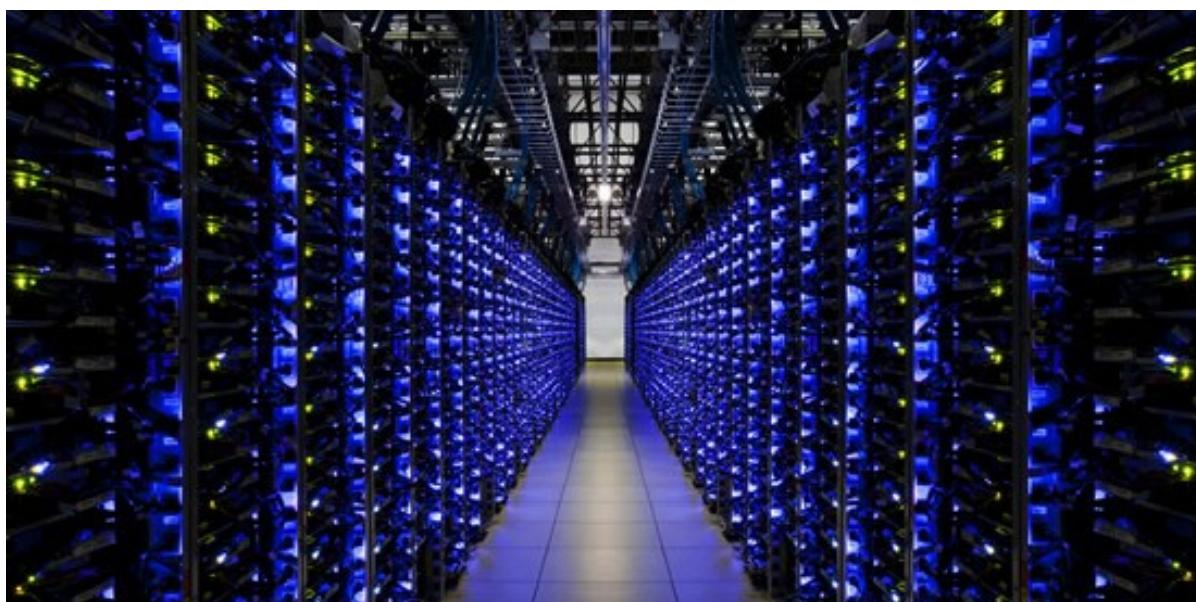


Figura 4. Exemple de CPD.

Com són els atacs?

Modus operandi

Quan parlem de ciberseguretat, parlem principalment d'atacs a la nostra infraestructura computacional i a la xarxa que la conté. Aquests atacs solen anar associats a un modus operandi per part dels atacants que els permet actuar de la manera més subtil i/o eficaç.

Les diverses tipologies d'atacant fan servir protocols que segueixen una estructura principal molt similar i difereixen en les eines o informació requerides per a l'atac. Per a informar-nos de les tècniques recomanem pegar una ullada a la Enterprise Matrix de MITRE ATT&CK®.

Per exemple, els APT (Advanced Persistent Threat) són grups d'infiltració sigil·losa en xarxa que es mantenen sense ser detectats durant un període prolongat i soLEN ESTAR patrocinats per algun estat. Això implica procedir amb la màxima discreció i fent el major reconeixement de xarxa possible per trobar els punts febles on fer-se persistents en secret.

D'altra banda, el crim organitzat busca crear disruptions o beneficis a partir d'un atac a una organització sense necessitat de quedar ocults ni tenir-ne persistència, motiu pel que les fases de reconeixement queden més diluïdes i es prioritza el robatori de dades.

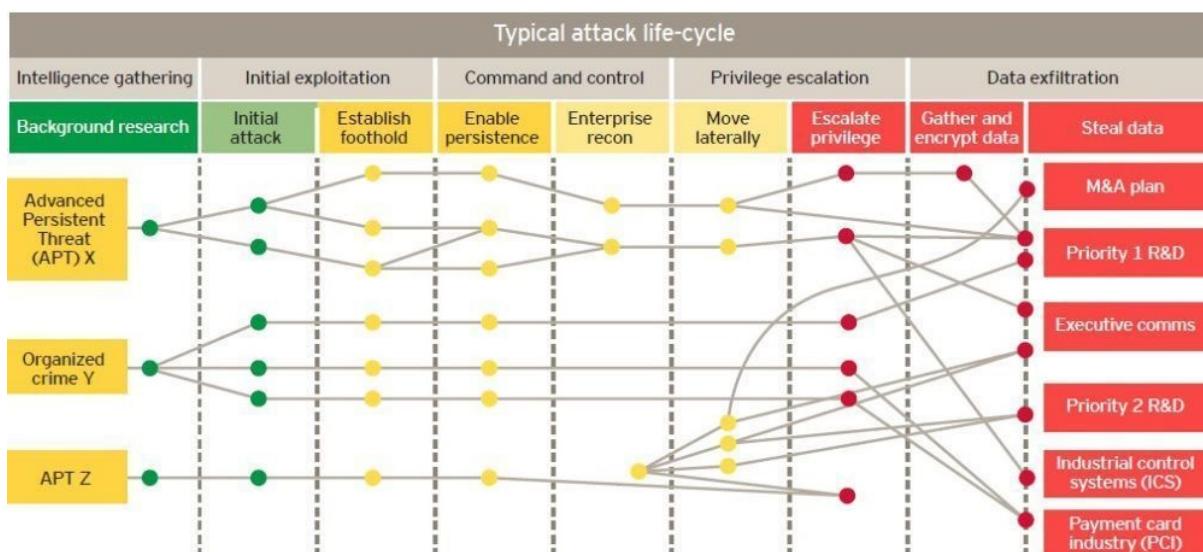


Figura 5. Fases típiques d'atacs.

Cal tenir en compte que els atacants fan servir accions malicioses de diverses ïndoles per poder realitzar totes aquestes activitats. Aquestes es coneixen en el món professional com a cyberthreats i n'existeixen diversos tipus que permeten classificar l'atac i respondre de la millor manera possible.

El modus operandi es veu directament afectat pel tipus d'atac que s'estigui efectuant, tal que un atac per malware pot implicar una automatització completa, però altres com el spear phishing requereixen de personalització o possible contacte directe amb la víctima, com passa amb el vishing.

Ciberamenaces més comuns

Existeixen diversos rànquing i tipologies de ciberamenaces que poden resultar d'interès quan ens preparem per a entrar en el món de la ciberseguretat. Entre ell destaquen alguns com OWASP Top Ten en el àmbit de les aplicacions web i OWASP Mobile Top 10, el seu derivat relatiu a les aplicacions mòbils.

La European Union Agency for Cybersecurity, anomenada ENISA pel seu nom previ (European Network and Information Security Agency), també genera el seu propi rànquing a nivell genèric i afegeix elements útils com informes relacionats que permeten aprofundir en l'estat actual i les tendències del ciberespai.

Dintre de les categories destacades per ENISA, el top 10 de 2020 són les següents:

#1 - Malware

El malware o programari maliciós inclou diverses famílies com els cryptominers, virus, ransomware, cucs i spyware. Els seus objectius comuns són el robatori d'informació o identitat, l'espionatge i la interrupció del servei.

Els costos associats al malware es basen en el propòsit d'aquest, per exemple, els criptominers (de les famílies més prevalents al 2019) implica uns alts costos de TI, un augment del consum d'electricitat i una reducció de la productivitat dels empleats. D'altra banda, el ransomware bloqueja completament l'accés a dades encriptant el disc o part d'aquest a forma de segrest fins que es pagui una quantitat (ransom). Per sort, el ransomware es manté a la part inferior de la llista de tipus de malware, però no cal oblidar el mal que pot causar en el sistema.

Per iniciar una difusió de malware, cal un vector d'entrada que sol ser per protocols web o per correu electrònic, però existeixen altres tècniques com la força bruta o l'aprofitament de vulnerabilitats mitjançant exploits que permeten arribar més enllà amb la difusió interna.

Cal destacar que en els últims anys s'ha produït un canvi notable d'objectius de malware, passant de atacat típicament als consumidors a atacar més sovint a les empreses.

#2 - Web-based Attacks

Els atacs basats en web són un mètode atractiu pel qual els actors de les amenaces poden enganyar les víctimes utilitzant sistemes i serveis web com a vector d'amenaces. Des de facilitar URL o scripts maliciosos per dirigir a la víctima al lloc web desitjat o a descarregar contingut maliciós, fins a injectar codi maliciós a un lloc web legítim compromès per a robar informació, obtenir beneficis financers o fins i tot per a l'extorsió mitjançant ransomware.

Els atacs de força bruta, per exemple, realitzen la seva operació desbordant una aplicació web amb intents d'inici de sessió amb contrasenya i nom d'usuari.

Els atacs basats en web poden afectar la disponibilitat de llocs web, aplicacions i interfícies de programació d'aplicacions (API), incomplint la confidencialitat i la integritat de les dades.

#3 - Phishing

El phishing és l'intent fraudulent de robar dades d'usuaris com ara credencials d'inici de sessió, informació de la targeta de crèdit o fins i tot diners mitjançant tècniques d'enginyeria social. Aquest tipus d'atac s'inicia generalment a través de missatges de correu electrònic, que sembla que s'envien des d'una font de bona reputació, amb la intenció de persuadir l'usuari perquè obri un fitxer adjunt maliciós o segueixi un URL fraudulent. Una forma específica de pesca anomenada "spear phishing" es basa en investigacions anticipades sobre les víctimes perquè l'estafa sigui focalitzada i aparegui més autèntica, cosa que la converteix en un dels tipus d'atac amb més èxit a les xarxes de les empreses.

El "Domain-based Message Authentication, Reporting, and Conformance" (DMARC) és un estàndard que garanteix que es bloquegi el correu electrònic de dominis fraudulents, disminuint la taxa d'èxit dels atacs de phishing, spoofing i spam.

En el futur, el correu electrònic continuarà sent el principal portador de phishing, però no per molt de temps. Estem veient recentment un augment de l'ús de la missatgeria en xarxes socials, WhatsApp i altres per realitzar atacs. El canvi més rellevant serà en els mètodes que s'utilitzen per enviar els missatges, que esdevindran més sofisticats amb l'adopció d'Intel·ligència Artificial (IA) per preparar i enviar els missatges. El phishing i el spear phishing són vectors principals d'atac d'altres amenaces, com ara insider threats.

#4 - Web Application Attacks

Les aplicacions i les tecnologies web s'han convertit en una part fonamental d'Internet adoptant diferents usos i funcionalitats. L'increment de la complexitat de les aplicacions web i els seus serveis generalitzats crea desafiaments per protegir-les contra amenaces. Els serveis i aplicacions web depenen principalment de bases de dades per emmagatzemar o lluir informació requerida.

El tipus d'atac SQL Injection (SQLi) és un exemple ben conegut i les amenaces més habituals contra aquests serveis. Els atacs de cross-site scripting (XSS) són un altre exemple. En aquest tipus d'atac, l'actor maliciós fa un mal ús de les debilitats dels formularis o d'altres funcionalitats d'entrada que condueixen a altres funcions malicioses, com ara ser redirigides a un lloc web maliciós.

#5 - Spam

Rebre correu brossa és un inconvenient, però també pot crear una oportunitat per a un actor maliciós de robar informació personal o instal·lar programari maliciós. El correu brossa consisteix a enviar massivament missatges no sol·licitats. Es considera una amenaça de ciberseguretat quan s'utilitza com a vector d'atac per distribuir o habilitar altres amenaces.

La principal diferència amb el phishing és que el spam no utilitza l'enginyeria social, sinó que actua sobre una llista massiva de correu. Les campanyes de correu brossa sempre han fet profit d'esdeveniments socials i esportius populars a nivell mundial, com ara la final de la UEFA Europa League o el US Open, entre d'altres. Tot i això, res en comparació amb la gran activitat de spam vist aquest darrer any amb la pandèmia COVID-19.

#6 - Denial Of Service

Se sap que es produeixen atacs de denegació de servei (DoS) o la seva versió distribuïda (DDoS) quan els usuaris d'un sistema o servei no poden accedir a la informació, serveis o altres recursos rellevants. Aquesta situació es pot aconseguir esgotant el servei o sobrecarregant els components de la infraestructura de xarxa. Històricament, els serveis DDoS s'anunciaven als fòrums de la dark web, però ara utilitzen canals de xarxes socials comuns com YouTube i Reddit per promocionar els seus serveis.

La implementació i la distribució de xarxes 5G augmentarà exponencialment el nombre de dispositius IoT connectats i, per tant, l'expansió de les xarxes de botnet, que en són el principal origen de trànsit DDoS.

#7 - Identity Theft

El robatori d'identitat o frau d'identificació és l'ús il·lícit de la informació d'identificació personal (PII) de la víctima per part d'un impostor per suplantar-la i obtenir un avantatge.

Segons un informe de seguretat anual, es van detectar almenys 900 casos internacionals de robatori d'identitat o delictes relacionats amb la identitat. Entre ells:

- Exposició de PII de ~106M de clients de banc de Capital One (març 2019).
- Exposició de 170M de comptes de la companyia de jocs Zynga (setembre 2019).
- Robatori de 20M de comptes del servei britànic Mixcloud (novembre 2019).
- Compromís de 600K conductors i 57M d'usuaris amb PII d'Uber (novembre 2019).
- Robatori de 9M de PII d'EasyJet, incloses targetes d'identitat i de crèdit (març 2020).

#8 - Data Breach

Un data breach és un tipus d'incident de ciberseguretat en el qual s'accedeix a la informació (o a una part d'un sistema d'informació) sense l'autorització adequada i que condueix a la pèrdua o ús indegit d'aquesta informació. També inclou un "error humà" que sovint es produeix durant la configuració i el desplegament de determinats serveis i sistemes, i que pot provocar una exposició involuntària de dades.

En molts casos, les empreses o organitzacions no són conscients que hi hagi un data breach. Segons es calcula, es necessiten uns 206 dies per identificar un data breach en una organització i sembla ser que l'impacte d'un data breach a nivell financer pot romandre durant més de 2 anys després de l'incident inicial.

Malgrat tots els riscos implicats, les organitzacions conserven cada cop més dades al núvol o en entorns locals complexos que estan gradualment més exposats a nous riscos.

#9 - Insider Threat

Una amenaça interna o insider threat és una acció realitzada per algú que treballa per a la empresa i que pot provocar un incident. En aquest sentit, hi ha diversos patrons associats com pot ser l'ús indegit de privilegis que es produeix quan els atacants col·laboren amb actors interns per obtenir accés als recursos.

Els interns, també coneguts com a privilegiats, poden causar danys sense voler i com que sovint gaudeixen de confiança, privilegis i coneixement del funcionament de l'empresa, és difícil distingir entre accés legítim, maliciós i erroni.

Els 5 tipus d'amenaca privilegiada es poden definir d'acord amb les seves raons i objectius:

- 1) Treballadors descuidats que manegen malament les dades, trenquen polítiques d'ús i instal·len aplicacions no autoritzades.
- 2) Agents interns que roben informació en nom de tercers.
- 3) Empleats descontents que intenten perjudicar la seva organització.
- 4) Privilegiats maliciosos que roben informació per obtenir beneficis personals.
- 5) Tercers que comprometen la seguretat via intel·ligència, ús indegit o accés maliciós.

Els cinc tipus d'amenaces s'han d'estudiar contínuament, ja que la seva existència hauria de definir part de l'estratègia de seguretat i protecció de dades de l'organització.

#10 - Botnet

Una xarxa de bot és una xarxa de dispositius connectats infectats per programari maliciós destinat a automatitzar una tasca. Aquests dispositius solen ser utilitzats per actors maliciosos per dur a terme atacs de denegació de servei distribuïts (DDoS).

Operant en un mode peer-to-peer (P2P) o des d'un centre de comandament i control (C2), les xarxes de bot són controlades remotament per un atacant de forma sincronitzada per obtenir un resultat determinat.

La informàtica i l'automatització han creat una oportunitat per a actors maliciosos per explorar noves tècniques i millorar les seves eines i mètodes d'atac. Gràcies a això, les xarxes bot funcionen de maneres molt més distribuïdes i automatitzades i estan disponibles als proveïdors d'autoservei i a punt per utilitzar.

Els bots maliciosos, anomenats "bad bots", no només evolucionen constantment, sinó que les habilitats de les persones i el nivell de desenvolupament dels bots s'estan especialitzant en certes aplicacions, com ara proveïdors de defensa o fins i tot tècniques d'evasió.

A més, aquestes xarxes de bots proporcionen un vector d'inici per a diverses operacions, des del frau de la banca electrònica fins al ransomware, la mineria de criptomonedes i els ja esmentats atacs DDoS.

Equips de seguretat

Els equips de seguretat estan present a tota empresa amb una mida considerable o que treballi amb dades que puguin necessitar un nivell de seguretat.

D'una banda, s'han de fer revisions periòdiques a les distintes bases de dades de vulnerabilitats i efectuar proves de penetració a la nostra xarxa corporativa i sistemes rellevants per tal de minimitzar-ne els riscos associats a l'explotació indeguda d'aquests. D'aquesta tasca se n'encarrega el que anomenem el **red team** o equip d'atac, que realitza operacions el més creatives possibles per descobrir els forats de seguretat que puguem tenir abans de que els descobreixi algú altre.

D'altra banda, els sistemes de hardware i software dels que disposem s'han de protegir i configurar adequadament per assegurar que no es pugui fer un mal ús dels recursos, ja siguin dades o computacionals. Aquesta és la missió del **blue team** o equip de defensa, que es compon tant de desenvolupadors de software, com de especialistes en xarxa o monitorització, entre altres.

Podem pensar que contractar un red team per fer l'anàlisi de seguretat de la nostra empresa és una mica infructuós si només ens diuen com han trencat la nostra seguretat però no ens ajuden a solucionar aquests forats, al igual que un blue team no ens és gaire útil si no sap pensar creativament com ho faria un atacant per saltar-se les mesures. Neix així el concepte de **purple team** o equip mixt, que posseeix qualitats tant de red com de blue per poder fer-ne un ús dels coneixements molt més efectiu.

Aquests tres equips soLEN fer servir sistemes operatius com ParrotOS i Kali Linux, tots dos basats en Debian, per fer la seva feina. Aquests sistemes estan dissenyats pensant en la seguretat i privacitat no només de l'usuari, sinó també de la seva feina, és a dir, que la seva configuració protegeix a l'usuari i facilita eines de treball en el món de la ciberseguretat que inclouen software per a proves de penetració, investigació de seguretat, informàtica forense i enginyeria inversa, però també inclou tot el necessari per desenvolupar el vostre propi programari o mantenir segures les vostres dades entre altres.

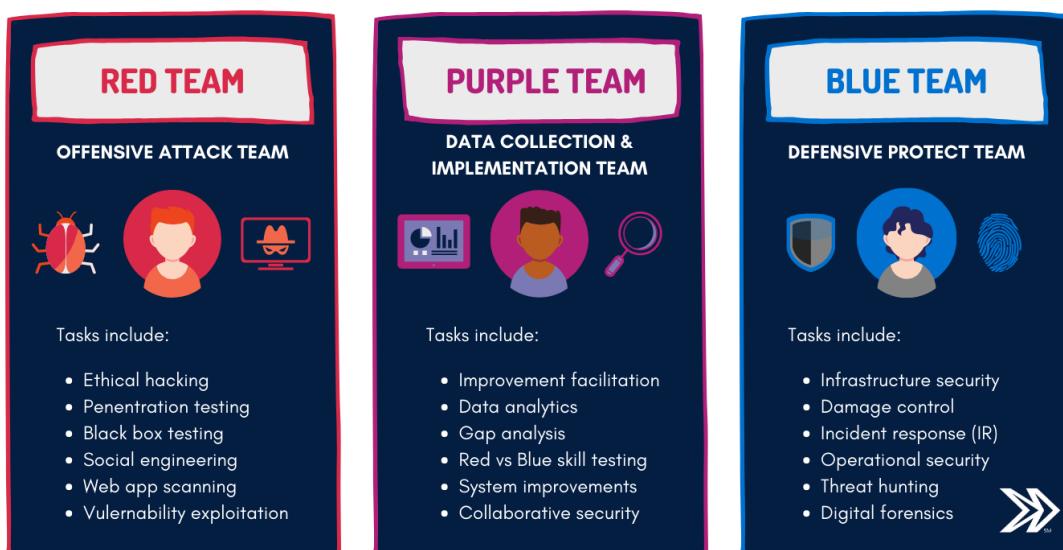


Figura 6. Tasques principals dels tres equips.

Red team (Atac)

Com ja hem introduït, el red team o equip d'atac s'encarrega de posar a prova els sistemes de que disposem per tal de trobar-ne forats de seguretat. Aquest equip sol venir de fora de la empresa i actua sota un contracte que determina clàusules de confidencialitat alhora que els límits i l'abast de les proves que es duran a terme.

Quan un red team es posa a la feina sol seguir una rutina d'atac que reflexa els moviments que faria qualsevol atacant. Per exemple:

Taula 1. Rutina d'atac d'un red team.

#	Escenari	Descripció
1	Reconeixement inicial	Aconseguir informació de l'empresa, treballadors i infraestructura i identificar-ne els elements vulnerables.
2	Compromís inicial	Emprar els vectors d'atac descoberts per saltar-se el perímetre de seguretat i accedir al sistema.
3	Establir punt de suport	Fortificar la posició obtinguda per a assegurar una re-entrada directa i treballar còmodament.
4	Escalar privilegis	Forçar el canvi a privilegis d'administrador saltant a un compte amb major autoritat per errors de configuració.
5	Reconeixement intern	Equivalent al 1er escenari però ja dins de la xarxa, resultant un reconeixement més profund.
5.1	Moviment lateral	Saltar a altres terminals de la xarxa per expandir-se internament i trobar més vectors d'atac.
5.2	Mantenir presència	Assegurar la re-entrada mitjançant backdoors per evitar que ens puguin fer fora amb petits contraatacs.
6	Missió completa	Efectuar l'atac corresponent (obtenir dades, bloquejar accés, etc.) i retirar-se del sistema.

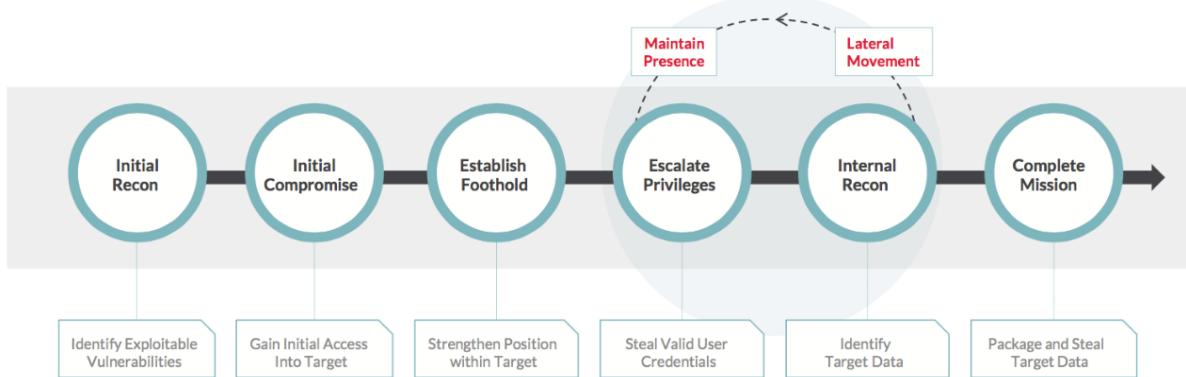


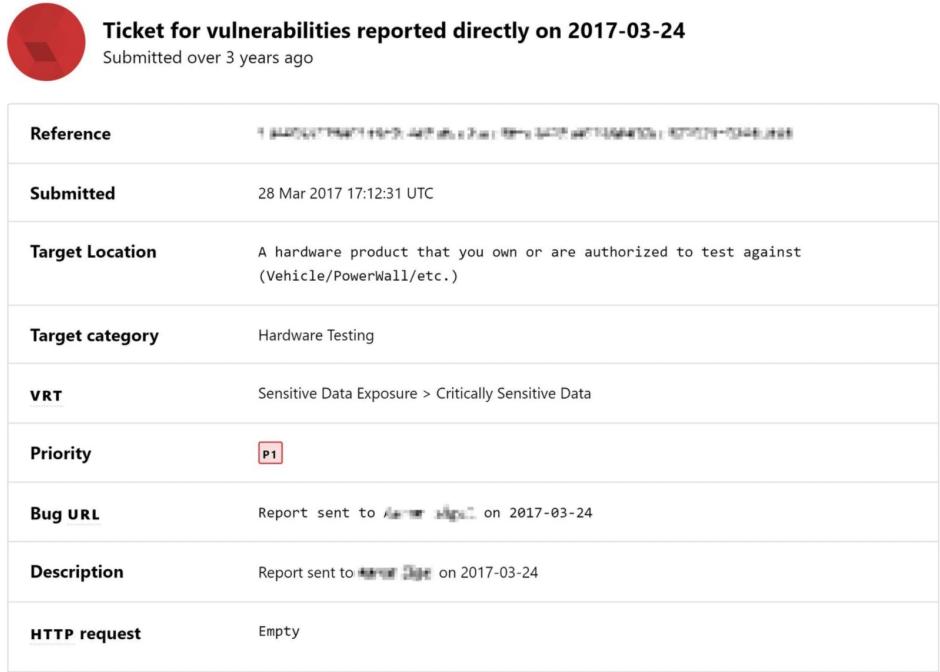
Figura 7. Rutina d'atac d'un red team.

La missió del red team és, per tant, detectar i contenir possibles intrusions per tal d'evitar que es produixin robatoris d'informació o disruptius en la operativa habitual de l'empresa. Per tal d'aconseguir-ho, el red team detecta els possibles punts febles de la companyia i ajuda a millorar els protocols de resposta davant d'un atac, tant entrenant a l'equip intern de la empresa com proporcionant informació de suport per als sistemes de monitorització i anàlisis de la infraestructura.

Una variant interessant dels red teams que està començant a popularitzar-se ara en els últims anys són els bounty hunters o caça-recompenses, individus que es registren en les bases de dades de seguretat de les empreses per a poder participar en els programes de recompensa per trobar errors en la seguretat d'aquestes.

Un exemple rellevant és el cas de Jason Hughes, un fanàtic de la comunitat de Tesla Motors que va prendre control de la flota sencera en Juliol de 2017. Com a membre de la comunitat interna, ja havia reportat altres vulnerabilitats en el passat però mai havia pogut arribar tant lluny. Segons l'informe presentat, Hughes va trobar un forat en el costat del servidor que permetia l'accés a les dades de tots els carregadors elèctrics de Tesla. A través d'aquest es va poder posicionar en el servidor i va aconseguir saltar fins al mothership, el servidor de l'empresa que permet comunicar-se amb la flota de cotxes. Un cop aquí, va prendre el control i va descobrir que podia donar l'ordre de conducció autònoma a qualsevol cotxe de la flota remotament i sense tenir-ne la propietat del mateix.

Així doncs, sembla evident que tenir un bon equip de professionals que ens facilitin detectar vulnerabilitats en el nostre sistema és primordial quan treballem en entorns on un atac qualsevol pot arribar a comportar grans conseqüències.



Ticket for vulnerabilities reported directly on 2017-03-24

Submitted over 3 years ago

Reference	11205477941974493633238893403483888
Submitted	28 Mar 2017 17:12:31 UTC
Target Location	A hardware product that you own or are authorized to test against (Vehicle/PowerWall/etc.)
Target category	Hardware Testing
VRT	Sensitive Data Exposure > Critically Sensitive Data
Priority	P1
Bug URL	Report sent to [REDACTED] on 2017-03-24
Description	Report sent to [REDACTED] on 2017-03-24
HTTP request	Empty

Status

Resolved

This submission has been fixed!

Reward

\$50,000

40 points

VRT version

1.0

Program

Tesla

Closed on

19 Apr 2017

Figura 8. Ticket de la vulnerabilitat de Jason Hughes per 50.000\$.

Eines de red team

Per poder fer la seva feina, el red team pot emprar milers d'eines especialitzades en distints escenaris que puguin donar-se. En aquest assaig no entrarem en detall en les eines del red team ni en farem un gran llistat d'aquestes, sinó que ens centrarem en destacar algunes de les eines més emprades, especialment en l'àmbit dels centres de processament de dades.

Eines de reconeixement actives

Les eines de reconeixement actives interactuen amb la xarxa afegint tràfic sobre aquesta i produint alteracions en el comportament habitual que poden arribar a ser detectades.

Una de les eines més emprades en aquest escenari és **Nmap**, que ens permet fer tasques com la detecció de ports oberts en hosts remots, el mapatge de xarxa i la enumeració de manera automatitzada i personalitzable. Un altre programa típic és **Nikto**, un software de escaneig de vulnerabilitats sobre servidors web que es pot fer servir paral·lelament a **sqlmap** per trobar també vulnerabilitats per injecció de SQL.

Cal tenir en compte en el món dels CPD que existeixen eines pensades per anàlisis a gran escala, com és el cas de **OpenVAS** (antigament anomenat Nessus) que ofereix diversos serveis i eines alhora per a escaneig de vulnerabilitats i la gestió d'aquestes, o de **Tsunami** (by Google), que ofereix múltiples plugins per detectar vulnerabilitats d'alta gravetat amb molta confiança.

Eines de reconeixement passives

Al contrari que amb les eines de reconeixement actives, les de caire passiu solen evadir la detecció buscant recursos en tercers implicats o escoltant la xarxa de manera promiscua.

Dins d'aquesta categoria es troben programes com **Wireshark** que analitza el tràfic en una xarxa i pot ajudar-nos a trobar problemes de configuració, però també programes de búsqueda d'informació capaços de fer-nos un perfil d'informació exposada de l'objectiu que estiguem estudiant. Aquest últim cas és el de **Spiderfoot** (by Steve Micallef), **Intrigue** (by Jonathan Cran) o **Maltego** (by Patreva), que automatizan la recerca de dades públiques i retornen informació que inclou noms, telèfons, correus, xarxes socials, noms de domini i adreces IP, relacions amb altres organitzacions, etc.

Al igual que amb les actives, existeixen eines de reconeixement passives com **OSINT Framework**, que inclou una solució completa per anàlisis de gran volum, o **Shodan**, que monitoritza la deep web i dispositius IoT públics i permet localitzar-los fàcilment.

Eines d'armamentització

Per poder executar els atacs i obtenir accés al sistema, els red teams solen emprar eines d'armamentització que els permeten explotar vulnerabilitats. En aquest sentit, eines com el **Social Engineering Toolkit (SET)** ens poden ajudar a crear atacs enfocats a les persones que inclouen phishing i correu en massa per verificar la feblesa dels treballadors, mentre que altres com **Metasploit** ens donaran el necessari per crear software d'atac que podem camuflar de persones amb **Invoke-Obfuscation** i de antivirus amb **Veil Framework**.

Eines de lliurament i explotació

Amb els atacs creats, els podem fer arribar a destí amb eines de lliurament com **Gophish** i **King Phisher** per via mail o directament a través del navegador si trobem algun error en el costat del client amb **BeEF**. Si amb això aconseguim capturar o accedir a algun fitxer de contrasenyes xifrat, podem fer ús de **Hashcat** o de **John The Ripper** per veure si és possible extreure algunes.

Eines d'escalada de privilegis

Si algun atacant aconsegueix arribar fins a aquí, podem començar a preocupar-nos. En aquest escenari pot decidir-se el grau de les conseqüències a les que pot arribar l'atac, doncs si s'adquireixen els privilegis adequats es podrà accedir a dades, sistemes i àrees que haurien de ser restringides. És, per tant, un punt crític del flux de l'atac.

Per a verificar si es poden escalar privilegis, trobem software específic com **PowerUp**, **BeRoot** o **BloodHound**, que busquen errades de configuració i exposen les llistes de control d'accés per poder visualitzar els camins disponibles per arribar per a distints usuaris i trobar la manera d'obtenir els privilegis desitjats.

Eines de moviment lateral

Per tal d'abrir la quantitat més gran possible de sistemes en la xarxa, el red team ha de realitzar moviments laterals per saltar amb eines com **Mimikatz**, que serveix per capturar o falsejar els credencials, o **LaZagne**, que extreu noms d'usuari i contrasenyes de diferents aplicacions.

Cal destacar l'existència de **CrackMapExec**, que ajuda aaprofitar Mimikatz per mapejar la xarxa i oferir les opcions de salt disponibles a les que podem arribar i executar **PAExec** per obtenir un terminal sense necessitat d'instal·lar software al destí.

Eines de comandament i control (C2)

Un cop arribats a aquest punt de la partida, el defensor té poca cosa a fer més que reaccionar a les conseqüències, doncs ara el red team pot establir les comunicacions persistents als sistemes controlats per tenir accés remot i establir túnels per a l'exfiltració de dades. Eines típiques de C2 són: **EvilURL**, **Empire Project**, **Pupy** o **Cobalt Strike**.

Eines d'exfiltració i finalització

Com a gran final de l'exercici, el red team pot extreure dades del sistema discretament amb tècniques d'exfiltració com poden ser l'ús de strings amb **Cloakify Factory**, la creació de peticions DNS amb **DNSExfiltrator**, la ocultació de dades en el protocol ICMP amb **DET** o fins i tot mitjançant fitxers adjunts a Gmail fent servir **Powershell-RAT**.

Com hem pogut veure, no només la seguretat interna dels nostres serveis és important. La seguretat física i la nostra informació a les xarxes públiques poden afectar significativament als inicis d'un atac que pot acabar greument segons com configurem i protegim elements clau del nostre sistema (contrasenyes, bases de dades, treballadors, ...). Existeixen molts factors que afecten a la seguretat i hem d'aconseguir protegir-nos el millor possible.

Blue team (Defensa)

El blue team, al igual que el red team, son equips de gent experta en ciberseguretat. La gent d'un blue team són especialistes en analitzar el comportament dels sistemes d'una empresa i el comportament dels usuaris i equips per detectar de forma ràpida qualsevol incident. A més, són els encarregats de fer la configuració de seguretat, com podria ser el firewall, ACL, VPN...

Es diu que el blue team és l'equip defensiu perquè són els encarregats de protegir des de dins, a diferència del red team que comprova aquestes defenses que posen els del blue.

L'objectiu del blue team es realitzar evaluacions de les diferents amenaces que poden afectar a l'empresa, monitoritzar i recomanar plans d'actuació per mitigar els riscos.

El blue team s'encarrega de documentar tot allò que interessa protegir, com dades sensibles o crítiques. Implementa polítiques per als treballadors i usuaris de l'empresa, com per exemple tindre contrasenyes més estrictes, i educa al personal perquè comprenguin i compleixin els procediments de seguretat i d'aquesta manera evitar que siguin atacats per estratègies com el phishing. També s'encarrega d'implementar eines que permeten que es registri la informació dels sistemes i així aconseguir veure comportaments inusuals.

El blue team realitza comprovacions periòdiques sobre el sistema de diversos tipus com podrien ser auditòries de DNS o captures de tràfic de xarxa.

Les funcions principals del blue team són: donar resposta a incidents, per contenir-los; threat hunting, que significa recerca activa d'amenaces; i solucions SIEM o EDR, que és molt important perquè avui dia els cibercriminals intentar trobar la forma de hakejar evitant les defenses tradicionals, així que és molt important detectar aquestes amenaces avançades. Un'altra responsabilitat del blue team són els anàlisis forenses, on estudien l'incident, rastrejen l'origen i avaluen l'impacte i l'abast d'aquest.

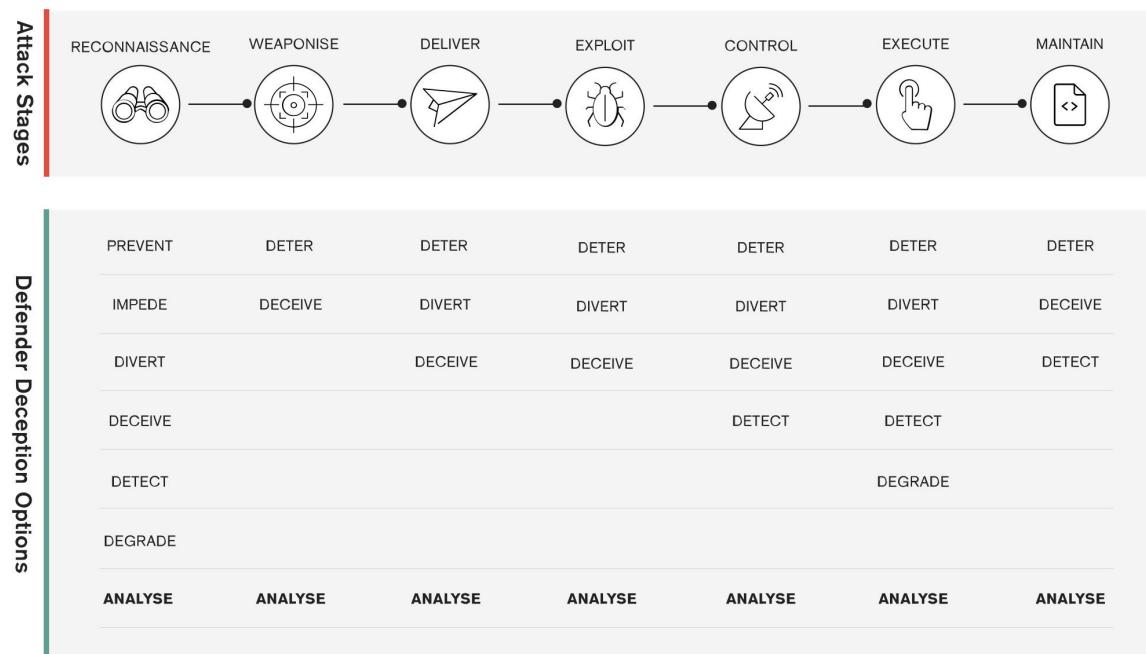


Figura 9. Opcions de defensa segons el tipus d'atac.

A més, el blue team està en constant evolució. Ha d'estar mirant les últimes tècniques de hakeig, ha de mirar les anàlisis de CVEs y vulnerabilitats 0-days constantment per poder definir alertes proactives i elaborar esquers.

Aquests esquers serveixen per atreure als intrusos però en realitat no suposa cap risc que ataquen a l'esquer. També utilitzen sandbox per provar codi maliciós sense perill.

Blue team es veu potenciat amb un red team, ja que el red team identifica les bretxes de seguretat amb les que el blue team optimitza la seva estratègia defensiva i monitoreig.

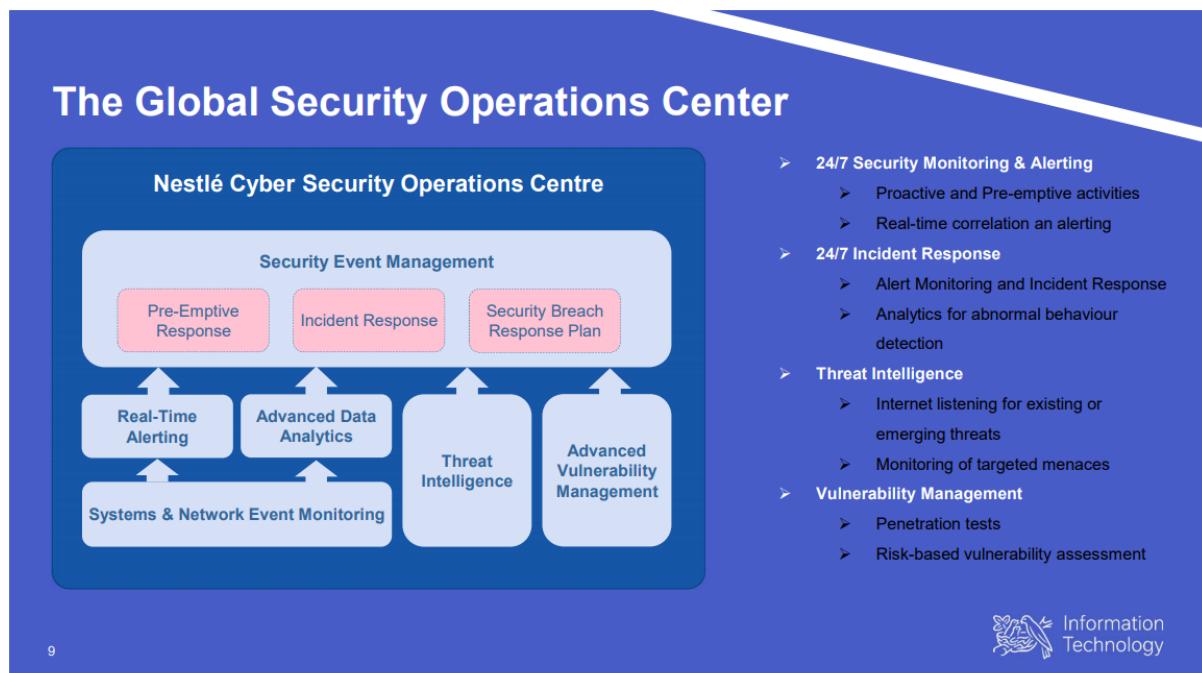


Figura 10. Exemple d'activitats del blue team de Nestlé.

En la imatge anterior tenim el que seria el blue team de Nestlé, també anomenat GSOC. La imatge descriu una mica l'activitat que té aquest GSOC. Com es pot veure, utilitza tot el que hem comentat amb anterioritat: busca noves amenaces emergents, avalua riscos de les vulnerabilitats, estan totes les hores del dia monitoritzant i fent activitats proactives, donen resposta a incidents a qualsevol hora i utilitzen threat intelligence el que engloba el threat hunting i el threat detection.

Eines de blue team

Com en tots els aspectes de la vida, en la ciberseguretat també existeixen eines i estratègies que faciliten l'activitat del blue team.

SIEMs

Les eines SIEM (Security Information and Event Management) utilitzen machine learning i big data. Aquestes eines recopilen informació en temps real de tota la infraestructura hardware i de les aplicacions en forma de logs, que son les dades en cru, i transforma aquests logs en dades més llegibles anomenades "events".

Tot i que un SIEM no és infal·lible, tenir-lo és un indicador clau de que una organització té definida una política important de ciberseguretat.

Les eines SIEM reuneixen diferents sistemes com els IDS (sistema de detecció d'intrusos) per donar una descripció completa de qualsevol incident.

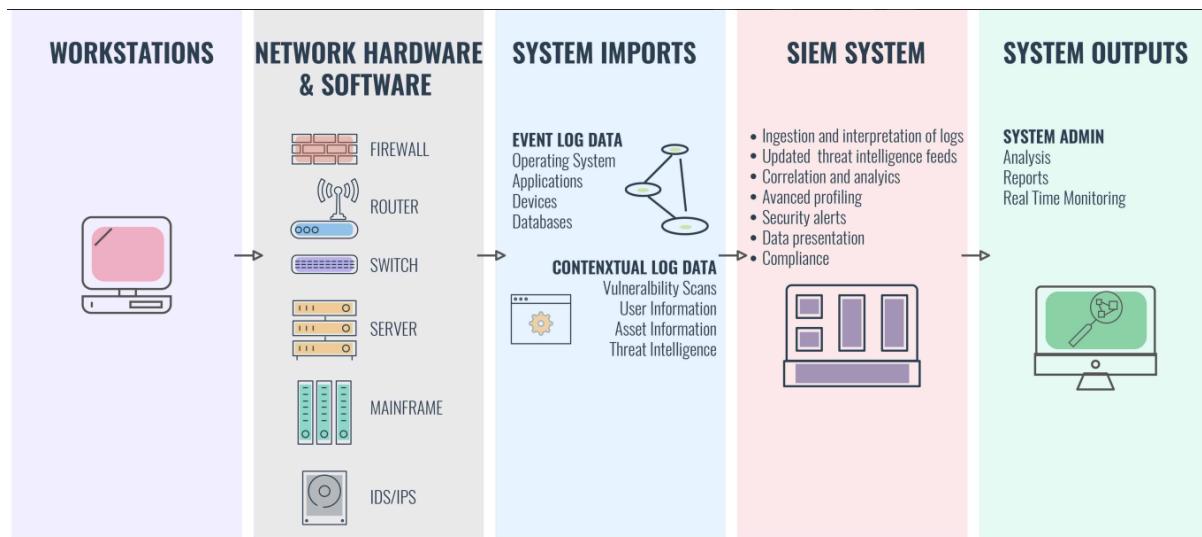


Figura 11. Disposició de defenses en un sistema.

Els SIEM s'han convertit cada cop més en un component principal en la seguretat de les organitzacions. La principal raó és que cada usuari deixa un rastre virtual en les dades de registre. Els sistemes SIEM estan dissenyats per utilitzar aquestes dades de registre i així generar informació sobre atacs i events passats. Els sistemes SIEM no només detecten l'atac, sinó que també permeten veure com i quan va ocórrer.

Alhora que l'entorn es va tornant més agressiu, contràriament a la creença popular, els firewalls i els paquets antivirus no són suficients per protegir una xarxa en la seva totalitat. Els atacs zero-day encara poden penetrar les defenses d'un sistema, fins i tot amb aquestes mesures de seguretat implementades.

Un SIEM aborda aquest problema detectant l'activitat d'atac i avaluant-la davant el comportament passat a la xarxa. Un sistema SIEM té la capacitat de distingir entre l'ús legítim i un atac malintencionat. Això ajuda a augmentar la protecció contra incidents d'un sistema i evitar danys als sistemes i la propietat virtual.

Algunes de les eines SIEM més completes i utilitzades:

- SolarWinds Security Event Manager
- Splunk
- OSSEC
- IBM QRadar SIEM
- McAfee Enterprise Security Manager

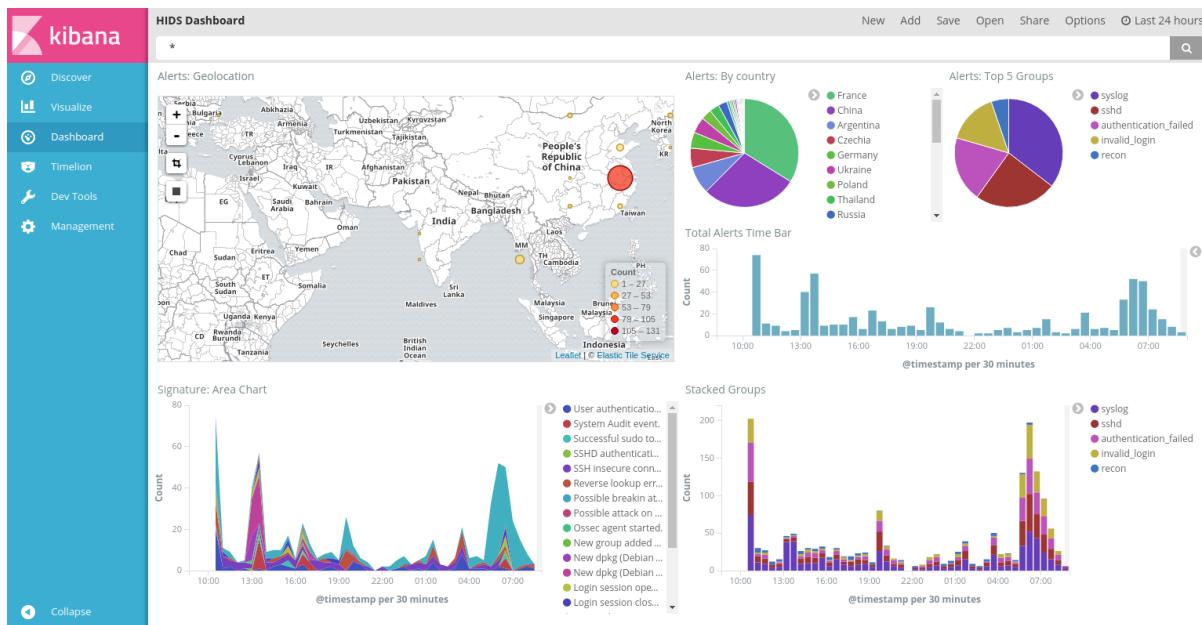


Figura 12. Exemple d'ús de l'eina OSSEC.

OSSIM

Parlem més a fons sobre OSSIM, un SIEM diferent a la resta que actualment és el més utilitzat del món.

OSSIM (Open Source Security Information Manager) és un SIEM que es va desenvolupar a l'any 2000. Aquest SIEM implementa la detecció i prevenció d'intrusos, i la seguretat de les xarxes en general. Aquest SIEM utilitza diverses eines conegeudes de monitorització i seguretat de codi obert. Gràcies a això ofereix un alt rendiment, donant com a resultat una intel·ligència capaç de traduir, analitzar i organitzar les dades d'una manera diferent a la resta de SIEMs.

L'arquitectura que té OSSIM és molt semblant a la de qualsevol SIEM: consta de 3 elements bàsics i un element extra per a la versió comercial.

Sensors: són els encarregats de recollir tota la informació del seu entorn local, processar-la i coordinar la detecció i resposta amb la resta de la xarxa OSSIM.

Col·lector: reuneixen els esdeveniments que generen els sensors i qualsevol sistema extern. Després classifiquen i normalitzen aquests esdeveniments abans d'enviar-los.

SIEM: proporciona capacitats d'intel·ligència i mineria de dades al sistema encarregat de la seguretat. En aquestes capacitats s'inclou: el control en temps real, indicadors de risc, anàlisis de vulnerabilitats i evaluació del risc.

Logger: aquest s'encarrega d'emmagatzemar els esdeveniments en un format RAW en un dispositiu de seguretat forense. Aquests esdeveniments s'emmagatzemen en massa i signats digitalment. Amb la signa s'aconsegueix que siguin admissibles com a prova en un tribunal.

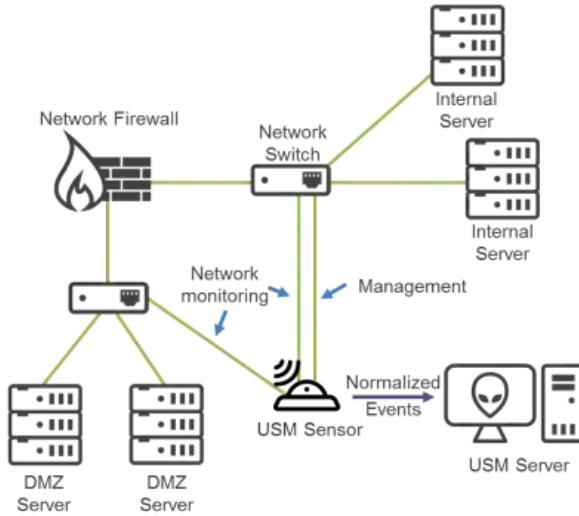


Figura 13. Arquitectura d'OSSIM.

OSSIM, com hem dit abans, està compost de diverses eines:

- **Snort:** Actualment és l'eina IDS open source més important. OSSIM conté una versió personalitzada y és aquesta eina la que avisa de possibles atacs a la xarxa.
- **Ntop:** un altre eina open source que s'encarrega de monitoritzar el tràfic de la xarxa. Aquesta eina proporciona informació important sobre el tràfic a la xarxa que ajuda a determinar si es tràfic anormal o maliciós de forma proactiva.
- **OpenVAS:** és la versió pública de Nessus, una coneguda eina d'escaneig de vulnerabilitats. Aquesta eina proporciona informació sobre les vulnerabilitats del recursos de xarxa i guarda aquesta informació a la base de dades d'OSSIM.

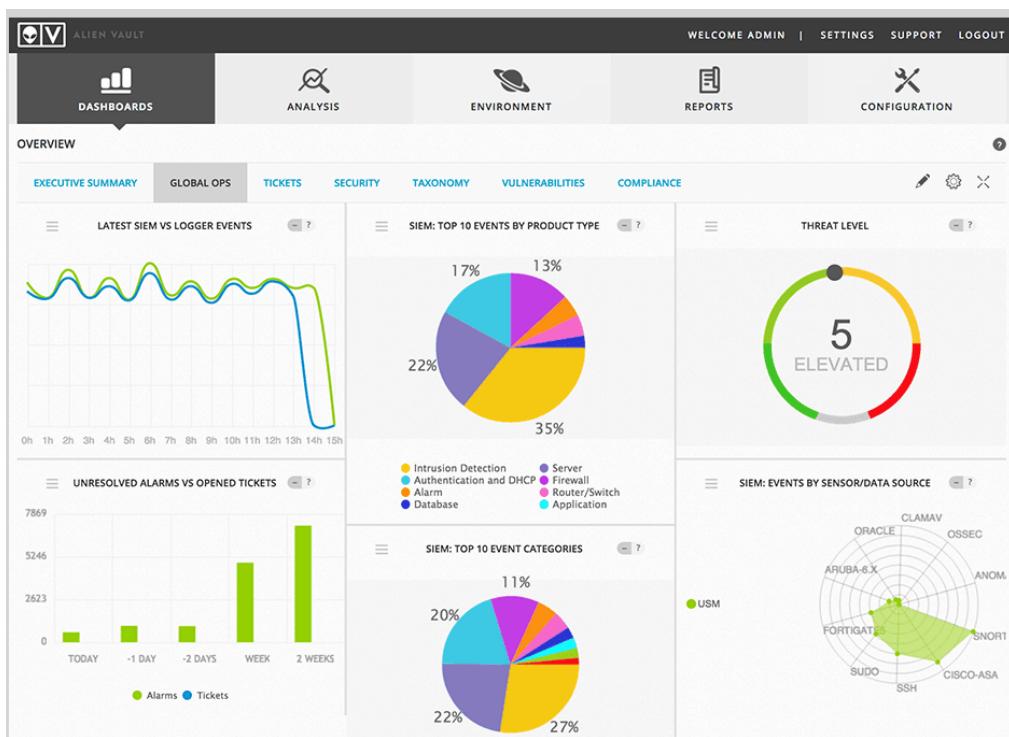


Figura 14. Captura de l'interfaç d'OSSIM.

Casos pràctics

Tot i que cada any es sol incrementar el pressupost per a seguretat en les empreses, no és suficient per assegurar que no pateixin cap atac informàtic.

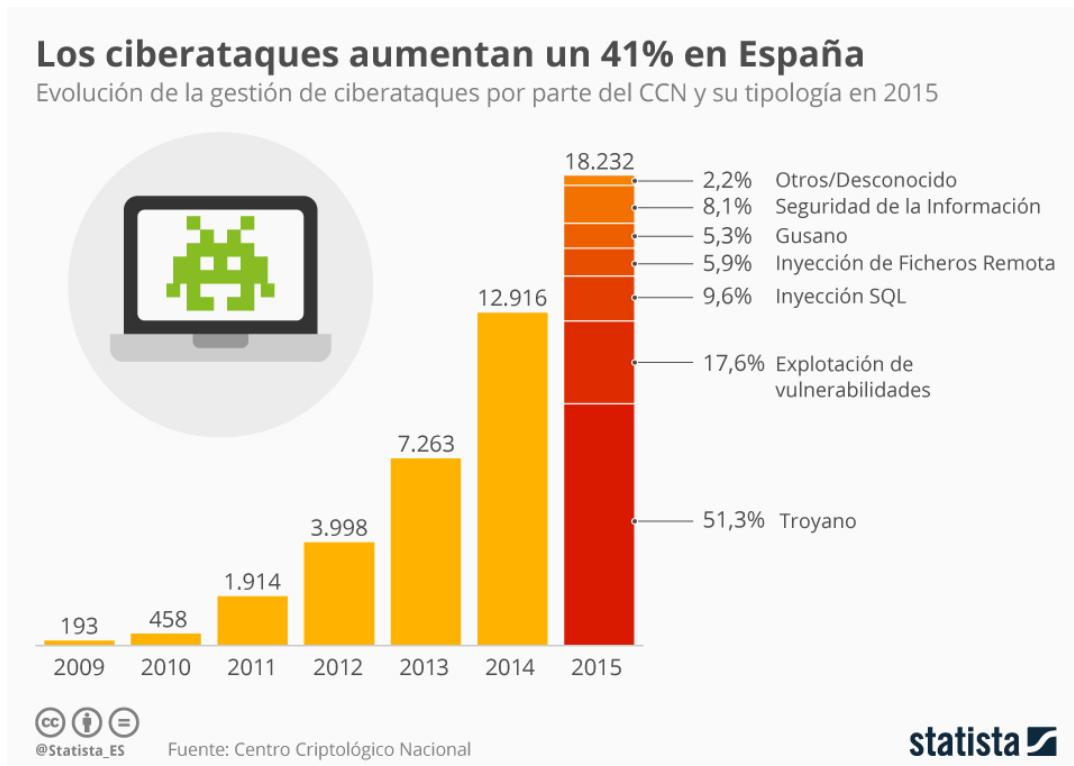


Figura 15. Gràfic de l'increment d'atacs informàtics a Espanya fins 2015

Com podem veure en la imatge anterior, tot i que el gràfic només arriba fins a 2015, es pot veure una realitat i es que cada any s'incrementen els casos d'atacs informàtics notablement.

Objectius dels hackers

Per començar aquests hackers pertanyen a la categoria black hat descrita al començament, ja que es dediquen a fer accions il·legals.

Atacs a grans empreses o multinacionals no son per res casualitat o mera curiositat per algun pirata informàtic.

Normalment l'objectiu principal dels hackers és aconseguir diners, aconseguir alguna mena de poder o avantatge i, en algunes ocasions, arribar a desacreditar l'empresa.

Com hem vist durant tot el document, hi han moltes maneres d'atacar, i entre les més utilitzades en parlarem d'entrades a través de troians o worms, en concret per a infiltrar un malware de categoria "ransomware" i/o per prendre control d'una xarxa i aconseguir exfiltrar-ne dades.

Cas 1. Adif

Adif és l'empresa pública que s'encarrega de gestionar la xarxa ferroviària. Aquesta empresa va ser atacada l'estiu de 2020 per el grup de cibercriminals anomenat "REvil", ells mateixos ho van fer públic a la seva pàgina web.

REvil es un grup de cibercriminals que utilitzant particularment el ransomware. Aquest grup ha fet diversos hakejos entre ells s'inclou un hakeig a un bufet d'advocats de grans celebritats com Lady Gaga, Madonna, Donald Trump...

The screenshot shows a blog post from the website 'adif.es'. The post is titled 'Adif (adif.es)'. It contains a warning message from REvil stating: 'Simultaneously with the publication, the third attack will follow. We advise you to get in touch immediately. We have personal information including correspondence, contracts and other accounting (total 800 gigabytes of data). If you do not comply with our terms, your data will be published in the public domain. We will continue to download your data until you contact us.' Below the message is a table titled 'RESUMEN CERTIFICACIONES EXP ON 007/11' showing a list of tax invoices (Certificaciones EXP) from January 2011 to August 2013. The table has columns for Num Certificación, Fecha, Total sin IVA, IVA, Importe IVA, and Importe.

Num Certificación	Fecha	Total sin IVA	IVA	Importe IVA	Importe
1	dic-11	294.947,35 €	18%	53.090,52 €	348.037,87 €
2	ene-12	10.434,45 €	18%	1.878,20 €	12.312,65 €
3	feb-12	53.305,34 €	18%	9.594,96 €	62.900,30 €
4	mar-12	53.801,83 €	18%	9.684,33 €	63.486,16 €
5	abr-12	97.393,88 €	18%	17.530,90 €	114.924,78 €
6	may-12	302.065,40 €	18%	54.371,77 €	356.437,17 €
7	jun-12	149.244,43 €	21%	31.341,33 €	180.585,76 €
8	jul-12	99.523,01 €	21%	20.899,83 €	120.422,84 €
9	ago-12	243.420,79 €	21%	51.118,37 €	294.539,16 €
10	sep-12	319.805,16 €	21%	67.159,08 €	386.964,24 €
11	oct-12	317.400,72 €	21%	66.654,15 €	384.054,87 €
12	nov-12	465.504,91 €	21%	97.756,03 €	563.260,94 €
13	dic-12	147.678,40 €	21%	31.012,46 €	178.690,86 €
14	ene-13	172.551,50 €	21%	36.235,82 €	208.787,32 €
15	feb-13	148.193,56 €	21%	31.120,65 €	179.314,21 €
16	mar-13	190.741,85 €	21%	40.055,79 €	230.797,64 €
17	abr-13	- €	21%	- €	- €
18	may-13	- €	21%	- €	- €
19	jun-13	- €	21%	- €	- €
20	jul-13	441.280,72 €	21%	92.668,95 €	533.949,67 €
21	ago-13	- €	21%	- €	- €

Figura 16. Missatge de REvil a la seva web.

El que va dir el grup REvil es que havien descarregat 800 GB en dades com contractes i comptabilitat. Van amenaçar a l'empresa dient que si no es posaven en contacte amb ells filtrarien tota la informació fent-la pública.

L'empresa va fer públic que va rebre un hakeig però no va fer pública la petició per el rescat de les dades ni si realment va estar compromesa tota la informació tot i que REvil diu que va fer públic 8 GB de 800 que van aconseguir.

Tot i que Adif va assegurar que va poder mantenir el sistema en el període del hakeig, està clar que van necessitar restaurar les dades dels backups i van perdre diners per tot el downtime encara que només fos per que el sistema no funcionava de la manera òptima.

Cas 2. FireEye

Dia 1 de desembre 2020. FireEye, una empresa de ciberseguretat amb seu a Califòrnia, va anunciar que va ser atacat de manera altament sofisticada i que es van robar eines de red team que poden suposar un perill per a moltes organitzacions a nivell mundial.

FireEye ha participat prèviament en la detecció i prevenció de ciberatacs importants i proporciona hardware, software i serveis per investigar atacs de ciberseguretat, protegir-se contra malware i analitzar els riscos de seguretat informàtics. No és d'estranyar que disposi de software especialitzat per verificar la seguretat d'una companyia.

Segons van anunciar, creuen que l'atacant pertany a un grup patrocinat per algun estat per la sofisticació, disciplina, seguretat operativa i les tècniques emprades en la operació.

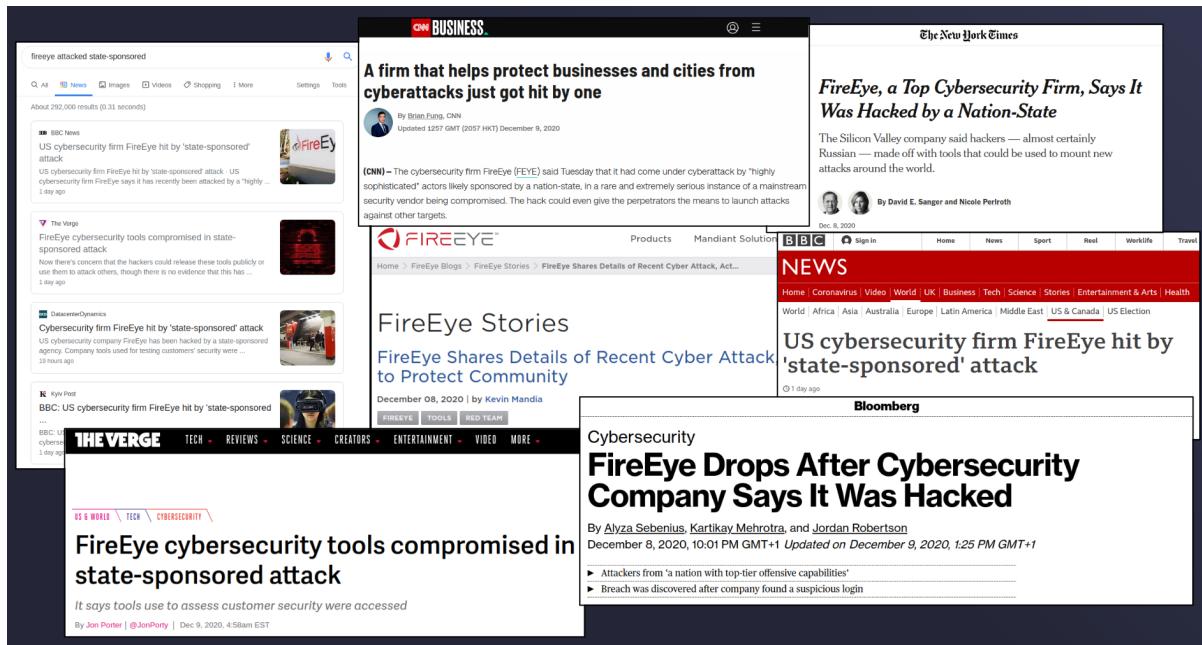


Figura 17. Col·lecció de notícies de l'atac a FireEye.

Què es va robar durant l'atac a FireEye?

D'acord amb les investigacions, l'atacant va buscar informació relacionada amb clients del govern. Tot i que l'atacant va poder accedir a alguns sistemes interns, en el moment de l'anunci, no hi havia proves de que els atacants haguessin exfiltrat (extret sense ser detectats) dades confidencials. Encara així, FireEye va confirmar que l'atacant havia accedit i robat les seves eines d'avaluació de red team.

Les eines robades van des de scripts de reconeixement fins a frameworks sencers que són similars a alguns de famosos com CobaltStrike i Metasploit. Moltes de les eines de red team ja s'han publicat i integrat a la màquina virtual de codi obert de FireEye: CommandoVM. El propòsit d'aquesta publicació és que qualsevol encarregat de seguretat o propietari de xarxa pugui verificar i resoldre la seguretat del seu sistema.

Per sort, el software robat no inclou vulnerabilitats zero-day (les que no s'han descobert en la comunitat i no han sigut reportades als desenvolupadors). Les eines robades apliquen mètodes coneguts i documentats que fan servir altres red teams de tot el món.

FireEye ha publicat una col·lecció de regles que ofereixen mesures contra les vulnerabilitats utilitzades en les seves eines de red team.

The screenshot shows the FireEye Stories blog post. At the top, there's a navigation bar with links to Products, Mandiant Solutions, and Customers. Below the navigation is a breadcrumb trail: Home > FireEye Blogs > FireEye Stories > FireEye Shares Details of Recent Cyber Attack, Act... The main title is "FireEye Stories" and the specific article title is "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community". The author is Kevin Mandia, and the date is December 08, 2020. There are three categories listed below the author: FIREEYE, TOOLS, and RED TEAM.

Figura 18. Publicació de detalls de l'atac per part de FireEye.

Per què va passar això?

L'anàlisi de FireEye va assenyalar una campanya d'intrusió mundial, un atac de la cadena de subministrament on s'incorporava un troià sobre les actualitzacions de software de l'empresa SolarWinds, que s'encarrega de desenvolupar programari utilitzat per agències federals i milers d'empreses privades per controlar les seves xarxes d'ordinadors.

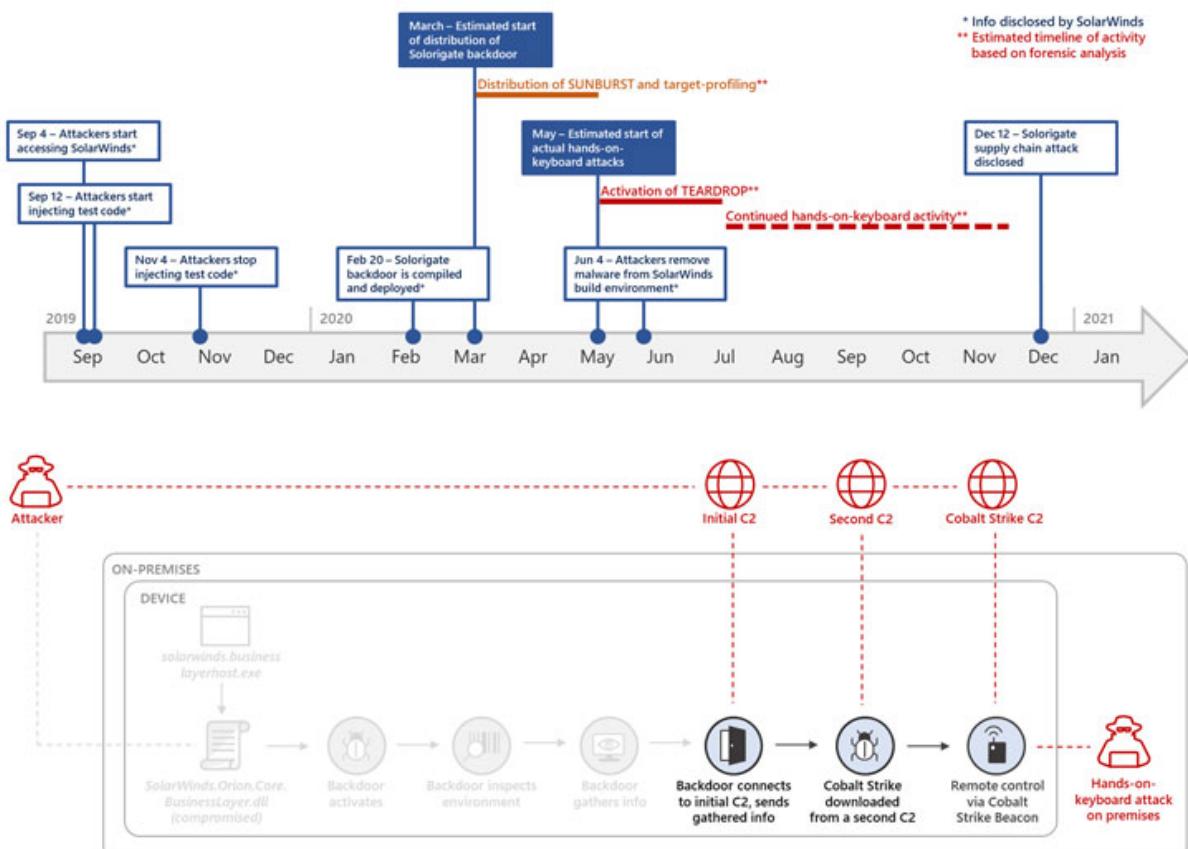


Figura 19. Cronologia de l'atac a SolarWinds.

Cas 3. SolarWinds

En base a investigacions de FireEye es va descobrir l'atac sobre l'eina Orion de SolarWinds, un software de seguretat que s'utilitza per a la gestió i supervisió de xarxes en moltes grans empreses i diverses agències governamentals dels Estats Units.

Els pirates informàtics, en lloc d'atacar directament els clients (grans empreses comptables, branques militars, ...) van decidir comprometre l'actualització automàtica del software per entrar de manera suau a milers de sistemes alhora. Així, els atacants van aconseguir obrir el pas a diverses xarxes on establir punt de suport per tal d'investigar vulnerabilitats estructurals i poder escalar privilegis i realitzar el reconeixement intern.

Prendent cura amb els detall, els atacants van aconseguir exfiltrar dades dels data center de sistemes governamentals dels Estats Units com el Departament del Tresor, el de Comerç i el de Seguretat Nacional, factor que els permetia veure el trànsit intern de correu electrònic.

Quin és l'impacte d'aquest atac?

Segons SolarWinds, 18.000 usuaris d'Orion han patit un data breach, incloses les empreses Fortune 500 i agències governamentals, fet que implica un cas d'espiatge estatal, i les empreses o institucions que han utilitzat actualitzacions infectades han de disconnectar els seus servidors i comprovar si han estat compromeses.

Segons FireEye, es tracta d'un atac patrocinat per algun estat i que anava dirigit a governs i empreses líders mundials, sobretot en els sectors de la tecnologia i l'energia a Amèrica del Nord, Europa, Àsia i Orient Mitjà.

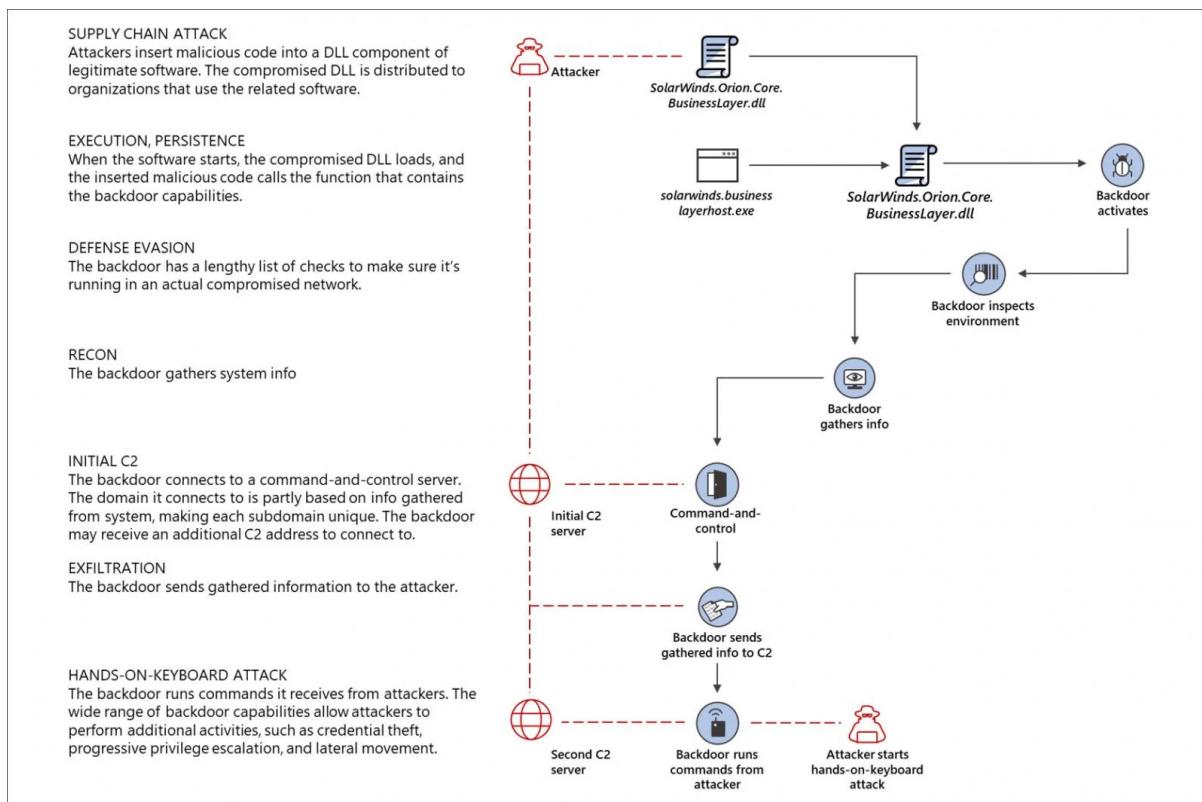


Figura 20. Modus operandi o rutina de l'atac a SolarWinds.

Cas 4. Microsoft Exchange

Encara que no s'ha trobat cap relació directa resulta curiós que l'atac a Microsoft Exchange tingüés lloc just després l'atac a SolarWinds.

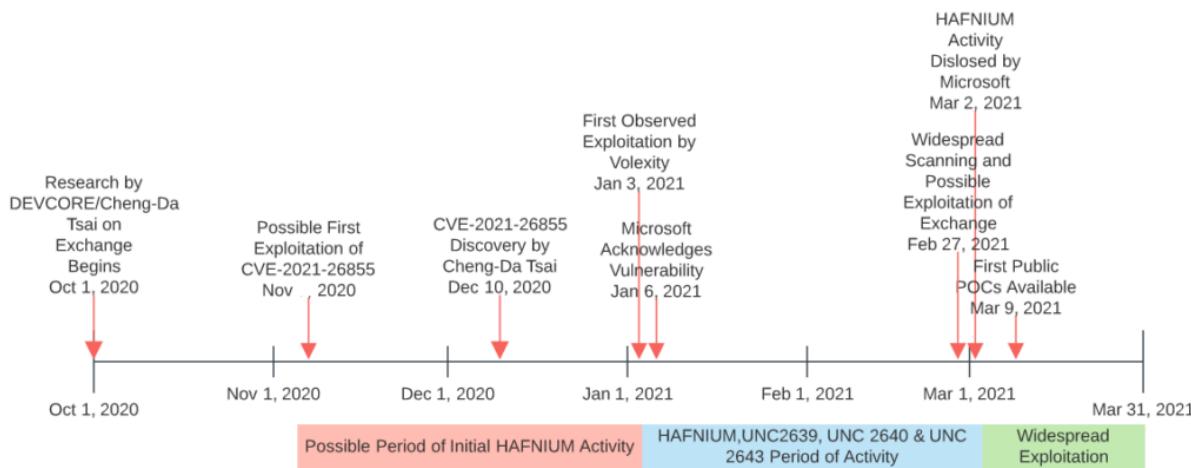


Figura 21. Cronologia de l'atac a Microsoft Exchange.

Aquest cas implica el descobriment de quatre errors zero-day a principis de gener de 2021, un d'ells valorat com a vulnerabilitat de 9.8 (risc crític) i els altres de 7.8 (risc elevat) sobre un màxim de 10. Segons sembla es van confirmar les vulnerabilitats i es va informar d'activitat sospitosa als servidors de Microsoft Exchange el mateix mes de gener.

El producte afectat en aquesta activitat era Microsoft Exchange Server, una solució de correu electrònic, calendari i col·laboració. Els usuaris d'aquest software cobreixen tot el rang des de petites i mitjanes empreses a gegants empresariais de tot el món.

Tot i que Microsoft ha publicat una actualització per corregir el problema, no tothom l'ha aplicat i el nombre de víctimes estimades continua creixent. L'extensió de l'atac és tal que ja s'han identificat més de 30.000 organitzacions afectades només als Estats Units.

Se sospita que els atacants disposen d'un codi PoC (Proof of Concept), emès de manera privada a socis i proveïdors de ciberseguretat, que els ha permès avançar-se a certes correccions per part de l'empresa i s'està estudiant la possibilitat d'una fuita accidental (o deliberada) que va provocar un augment en atacs. Aquest fet ens fa preguntar-nos: quina possibilitat hi ha que aquest PoC fos robat a alguna entitat en l'atac a Orion de SolarWinds?

CVE-2021-26855 Detail

Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-27078.

Severity	CVSS Version 3.x	CVSS Version 2.0
NVD	NIST: NVD	Base Score: 9.8 CRITICAL
		Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Figura 22. Detall de la vulnerabilitat crítica CVE-2021-26855.

Bibliografia

- [1] "What is the Difference Between Black, White and Grey Hat Hackers?" [Online]. Available: <https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html>
- [2] "Origen e importancia de la ciberseguridad," Sep. 2020. [Online]. Available: <https://openwebinars.net/blog/origen-e-importancia-dela-ciberseguridad/>
- [3] "How Secure is Your Password? - gHacks Tech News." [Online]. Available: <https://www.ghacks.net/2012/04/07/how-secure-is-your-password/>
- [4] "Seguridad en cpd," 2021. [Online]. Available: <https://www.aui.es/IMG/ponencia2349.pdf>
- [5] "Matrix - enterprise — mitre attck®." [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>
- [6] "Cyber attack life cycle," 2021. [Online]. Available: <https://aristininja.com/cyber-attack-life-cycle/>
- [7] "Cyber Attack - What Are Common Cyberthreats?" [Online]. Available: <https://www.cisco.com/c/en/us/products/security/commoncyberattacks.html>
- [8] "OWASP Top Ten Web Application Security Risks | OWASP." [Online]. Available: <https://owasp.org/www-project-top-ten/>
- [9] "OWASP Mobile Top 10." [Online]. Available: <https://owasp.org/wwwproject-mobile-top-10/>
- [10] "Threat Landscape." [Online]. Available: <https://www.enisa.europa.eu/topics/threat-risk-management/threatsand-trends>
- [11] "ENISA Threat Landscape 2020 - Malware." [Online]. Available: <https://www.enisa.europa.eu/publications/malware>
- [12] "ENISA Threat Landscape 2020 - Web-based attacks." [Online]. Available: <https://www.enisa.europa.eu/publications/web-based-attacks>
- [13] "ENISA Threat Landscape 2020 - Phishing." [Online]. Available: <https://www.enisa.europa.eu/publications/phishing>
- [14] "ENISA Threat Landscape 2020 - Web application attacks." [Online]. Available: <https://www.enisa.europa.eu/publications/web-applicationattacks>
- [15] "ENISA Threat Landscape 2020 - Spam." [Online]. Available: <https://www.enisa.europa.eu/publications/spam>
- [16] "ENISA Threat Landscape 2020 - Distributed denial of service." [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threatlandscape-2020-distributed-denial-of-service>
- [17] "ENISA Threat Landscape 2020 - Identity Theft." [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape2020-identity-theft>
- [18] "ENISA Threat Landscape 2020 - Data Breach." [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape2020-data-breach>
- [19] "ENISA Threat Landscape 2020 - Insider Threat." [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape2020-insider-threat>
- [20] "ENISA Threat Landscape 2020 - Botnet." [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape2020-botnet>
- [21] S. Climer, " USRed Team Vs Blue Team: The Two Sides Of Cybersecurity: A Cybersecurity Report | Mindsight," Jun. 2020. [Online]. Available: <https://gomindsight.com/insights/blog/red-team-vs-blue-team/>

- [22] B. Gonzalez, “¿Es lo mismo Red Team y Blue Team? | Hard2bit CyberSecurity.” [Online]. Available: <https://hard2bit.com/blog/red-temvs-blue-team/>
- [23] “¿Quién es quién en ciberseguridad y hacking? | Basetis now!” [Online]. Available: <https://blog.basetis.com/es/content/quien-es-quien-en-ciberseguridad-y-hacking>
- [24] “Red Team - Servicios de Red Teaming | Ciberseguridad - Tarlogic.” [Online]. Available: <https://www.tarlogic.com/blackarrow-servicios-seguridadofensiva/red-team/>
- [25] F. Lambert, “The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he’s a good guy,” Aug. 2020. [Online]. Available: <https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/>
- [26] “SecurityTrails | Top 30+ Most Popular Red Team Tools.” [Online]. Available: <https://securitytrails.com/blog/red-team-tools>
- [27] “Auditoría Web - Enfoques para el estudio de seguridad Web.” [Online]. Available: <https://www.tarlogic.com/blackarrow-servicios-seguridadofensiva/blue-team/>
- [28] “What can Deception do to Defend Across the Attack Lifecycle?” Aug. 2018. [Online]. Available: [/blog/post/deception-technology-defend-acrossattack-lifecycle/](https://blog/post/deception-technology-defend-acrossattack-lifecycle/)
- [29] “AI for security monitoring and alerting,” Nov. 2020.
- [30] “10 Best SIEM Tools of 2021: Vendors & Solutions Ranked (Paid & Free),” Feb. 2019. [Online]. Available: <https://www.comparitech.com/netadmin/siem-tools/>
- [31] A. Chalothorn, “OSSEC Thai Open Source.” [Online]. Available: <https://thaiopensource.org/%e0%b8%a1%e0%b8%b2%e0%b9%80%e0%b8%a5%e0%b9%88%e0%b8%99-oss-ec-%e0%b8%81%e0%b8%b1%e0%b8%99/>
- [32] “OSSIM: The Open Source SIEM | AlienVault.” [Online]. Available: <https://cybersecurity.att.com/products/ossim>
- [33] “About Network IDS (NIDS) in AlienVault USM Appliance.” [Online]. Available: <https://cybersecurity.att.com/documentation/usmappliance/ids-configuration/about-alienvault-nids.htm>
- [34] S. N. Company, “Sudo Null - Latest IT News.” [Online]. Available: <https://sudonull.com/post/99501-OSSIM-deploying-a-comprehensive-open-source-security-management-system>
- [35] “Infografía: Los ciberataques en España.” [Online]. Available: <https://es.statista.com/grafico/6876/los-ciberataques-en-espana/>
- [36] A. R. Aguiar, “Adif, víctima de un ataque informático del mismo grupo de cibercriminales que hackeó a los abogados de Trump: aseguran haber robado 800 GB de datos,” Jul. 2020. [Online]. Available: <https://www.businessinsider.es/adif-victima-ciberataque-hanrobado-800gb-datos-682565>
- [37] P. G. o. December 17 and 2020, “FireEye Hack Turns into a Global Supply Chain Attack,” Dec. 2020. [Online]. Available: <https://securityboulevard.com/2020/12/fireeye-hack-turns-into-a-global-supply-chain-attack/>
- [38] “How A Cybersecurity Firm Uncovered The Massive Computer Hack.” [Online]. Available: <https://www.npr.org/2020/12/21/948843356/how-a-cybersecurity-firm-uncovered-the-massive-computer-hack>
- [39] “FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community.” [Online]. Available: <https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html>
- [40] “Here’s How SolarWinds Hackers Stayed Undetected for Long Enough.” [Online]. Available: <https://thehackernews.com/2021/01/hereshow-solarwinds-hackers-stayed.html>

- [41] "The SolarWinds cyberattack: The hack, the victims, and what we know." [Online]. Available: <https://www.bleepingcomputer.com/news/security/the-solarwindscyberattack-the-hack-the-victims-and-what-we-know/>
- [42] "Data crunching consequences of SolarWinds cyberattack." [Online]. Available: <https://techxplore.com/news/2020-12-unquantified-consequencesolarwinds-cyberattack.html>
- [43] Alejandro, "Protegerse de las vulnerabilidades ProxyLogon en Microsoft Exchange," Mar. 2021. [Online]. Available: <https://protegermipc.net/2021/03/16/vulnerabilidades-proxylogonmicrosoft-exchange/>
- [44] "NVD - CVE-2021-26855." [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2021-26855>
- [45] "NVD - CVE-2021-26857." [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2021-26857>
- [46] "NVD - CVE-2021-26858." [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2021-26858>
- [47] "NVD - CVE-2021-27065." [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2021-27065>
- [48] C. Osborne, "Everything you need to know about the Microsoft Exchange Server hack." [Online]. Available: <https://www.zdnet.com/article/everything-you-need-to-know-aboutmicrosoft-exchange-server-hack/>
- [49] "Microsoft Exchange Hack Could Be Worse Than SolarWinds," Mar. 2021. [Online]. Available: <https://www.datacenterknowledge.com/security/microsoftexchange-hack-could-be-worse-solarwinds>
- [50] "At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software — Krebs on Security." [Online]. Available: <https://krebsonsecurity.com/2021/03/at-least-30000-us-organizations-newly-hacked-via-holes-in-microsofts-email-software/>