ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Phishing i bones pràctiques

Juny 2023

ÍNDEX

1. Introducció

Després dels últims incidents , principalment basats en phishing, dels quals s´ha detectat un augment del nombre d´atacs , de forma molt dirigida, però sobretot molt especialitzada, pel que fa a la "mutació" del "modus operandi".

Això es deu a que cada cop més, les organitzacions disposen d´elements de protecció més avançats, per la qual cosa es busca el vector d´entrada més dèbil, que acostuma a ser l´usuari final del servei.

A nivell d'intel·ligència, si que es nota que dins aquestes campanyes, s´està utilitzant cada cop més la IA (intel·ligència artificial), el que fa que sigui molt complicat establir patrons de conducta recurrents.

2. Que es el phishing

El phishing és una tècnica d'enginyeria social utilitzada pels ciberdelinqüents per obtenir informació confidencial de manera fraudulenta. Consisteix a enviar missatges falsificats, ja sigui per correu electrònic, missatges de text, o fins i tot a través de xarxes socials, fent-se passar per una entitat legítima , una empresa o una institució governamental.

L'objectiu principal del phishing és enganyar les víctimes perquè revelin informació personal, com contrasenyes, números de targetes de crèdit, dades personals o altra informació sensible. Aquests estafadors es fan passar per una entitat de confiança i demanen a la persona que realitzi una acció específica, com fer clic en un enllaç, descarregar un arxiu adjunt o proporcionar les seves dades personals en un formulari fals.

L'èxit del phishing rau en la seva capacitat per enganyar les persones. Els missatges de phishing solen estar dissenyats de manera molt convincent, utilitzant logotips, colors i llenguatge similar al de l'entitat que estan suplantant. També poden utilitzar tàctiques d' urgència o amenaces per pressionar la víctima a prendre acció immediatament, sense tenir temps per qüestionar l' autenticitat del missatge.

Una vegada que la víctima cau en el parany i proporciona la informació sol·licitada, els estafadors la utilitzen per cometre frau , robatori d'identitat o altres delictes cibernètics. Poden accedir a comptes bancaris, comptes de xxss o altres dades, realitzar transaccions no autoritzades o vendre la informació en el mercat negre.

3. Gestió segura de credencials; protegint la informació sensible

En l'era digital actual, on gran part de les nostres activitats diàries es realitzen en línia, la gestió segura de credencials s'ha tornat més crucial que mai. Les credencials, com contrasenyes i noms d'usuari, són les claus que ens permeten accedir als nostres

comptes en línia, des de xarxes socials fins a altres serveis. Per tant, protegir aquestes credencials és fonamental per garantir la seguretat de la nostra informació personal i evitar l' accés no autoritzat als nostres comptes.

Una de les pràctiques més importants en la gestió de credencials és utilitzar contrasenyes segures. Una contrasenya segura ha de ser única i complexa, la qual cosa significa que no ha de ser fàcil d' endevinar i ha d' incloure una combinació de lletres, nombres i caràcters especials. Evita utilitzar informació personal òbvia, com el teu nom, data de naixement o números de telèfon, ja que aquestes dades són fàcils d'obtenir per als atacants.

A més, és essencial que cada compte tingui una contrasenya diferent. Tot i que pot ser temptador utilitzar la mateixa contrasenya per a múltiples comptes, això augmenta significativament el risc que un atacant accedeixi a tots els teus comptes si una sola contrasenya és compromesa. Utilitzar un gestor de contrasenyes confiable pot ajudar-te a generar i emmagatzemar contrasenyes segures per a cada compte de manera segura.

Un altre aspecte important en la gestió de credencials és l'autenticació de dos factors (2FA). Aquesta capa addicional de seguretat requereix un segon factor, a més de la contrasenya, per verificar la identitat de l' usuari. Pot ser un codi únic enviat al teu telèfon mòbil, una empremta dactilar o un token de seguretat. L'autenticació de dos factors dificulta enormement als atacants accedir als teus comptes fins i tot si coneixen la teva contrasenya.

La gestió segura de credencials també implica evitar compartir les teves contrasenyes amb altres persones. És comprensible que hi pugui haver situacions en què necessitis compartir accés a un compte amb un membre de confiança de la teva família o un col·lega, però assegura't de fer-ho de forma segura, per exemple, compartint la contrasenya de forma personal i no a través de canals insegurs com correu electrònic o missatges de text.

A més, has d'estar atent als possibles atacs de phishing. Els atacants sovint intenten obtenir credencials mitjançant l'enviament de correus electrònics o missatges fraudulents que semblen provenir de llocs legítims. Aquests missatges demanen que ingressis les teves credencials en llocs web falsificats, cosa que els permet als atacants obtenir accés als teus comptes. Per evitar caure en aquestes trampes, verifica sempre l'autenticitat dels correus electrònics i els enllaços abans de proporcionar qualsevol informació.

Finalment, és important mantenir les teves credencials actualitzades i revisar regularment les activitats en els teus comptes. Canvia les teves contrasenyes de forma periòdica i mantenen un registre dels serveis en els quals estàs registrat per poder fer un seguiment dels teus comptes en línia. Si notes activitat sospitosa o no reconeguda, actua immediatament i comunicat amb el proveïdor de serveis corresponent.

4. La instal·lació de malware a través del phishing: Una amenaça persistent en l'era digital

En l'actualitat, el phishing continua sent una de les tècniques més comunes i efectives utilitzades pels ciberdelinqüents per distribuir malware i comprometre la seguretat dels usuaris en línia. El terme "phishing" es refereix a la pràctica d'enviar correus electrònics, missatges o comunicacions fraudulentes que es fan passar per entitats legítimes per tal d'enganyar les víctimes i obtenir informació confidencial.

Una de les principals conseqüències del phishing és la instal·lació de malware en els sistemes de les víctimes. El malware és un programari maliciós dissenyat per danyar, infectar o accedir de manera no autoritzada a un sistema informàtic. Un cop el ciberdelinqüent enganya la víctima perquè obri un arxiu adjunt, faci clic en un enllaç o proporcioni informació confidencial, s'activa el procés d'instal·lació del malware.

Els ciberdelinqüents utilitzen diverses tàctiques per convèncer les víctimes que realitzin accions que permetin la instal·lació de malware. Poden enviar correus electrònics que semblen provenir d'una entitat de confiança, una empresa reconeguda, un lloc de compra en línia, sol·licitant que es faci clic en un enllaç per actualitzar dades o canviar contrasenyes. En fer clic en aquest enllaç, la víctima pot ser redirigida a un lloc web fals que imita l'aparença del lloc legítim, però en realitat està dissenyat per infectar el seu sistema amb malware.

Una altra tàctica comuna és l'enviament d'arxius adjunts maliciosos. Aquests arxius poden estar disfressats de documents legítims, com factures, currículums o arxius PDF. En obrir l'arxiu adjunt, s'activa el malware i comença a executar-se en el sistema de la víctima sense el seu coneixement. Aquest malware pot robar informació confidencial, registrar pulsacions de tecles, controlar la càmera o el micròfon del dispositiu i permetre l'accés remot al sistema.

La instal·lació de malware a través del phishing pot tenir greus conseqüències per als usuaris i les organitzacions. Pot portar al robatori de dades sensibles, com informació financera, contrasenyes i dades personals. A més, el malware pot ser utilitzat per llançar atacs addicionals, com l'enviament massiu de correus no desitjats, el segrest de comptes o el xifrat d'arxius per exigir un rescat.

Per protegir-se contra la instal·lació de malware a través del phishing, és important seguir algunes mesures de seguretat. En primer lloc, és fonamental tenir precaució en obrir correus electrònics o missatges sospitosos. Presta atenció als remitents desconeguts o correus electrònics que semblen fora del comú, i evita fer clic en enllaços o descarregar arxius adjunts de fonts no confiables.

5. Altres amenaces relacionades

Smishing, Vishing i Carding: Les amenaces emergents en l'era digital.

En l'era digital actual, on la tecnologia s'ha tornat omnipresent, els ciberdelinqüents estan constantment evolucionant les seves tàctiques per explotar noves vulnerabilitats i enganyar els usuaris desprevinguts. Entre les amenaces emergents es troben l'smishing, el vishing i el carding, tècniques que busquen obtenir informació confidencial i cometre frau financer.

L'smishing és una combinació de "SMS" i "phishing". En aquesta tècnica, els atacants envien missatges de text falsificats als dispositius mòbils de les víctimes, fent-se passar per entitats legítimes o proveïdors de serveis. Aquests missatges demanen a la víctima que realitzi una acció específica, com proporcionar informació personal o fer clic en un enllaç maliciós. L'objectiu és enganyar la persona perquè reveli dades confidencials que els ciberdelinqüents utilitzaran per cometre frau.

El vishing, d'altra banda, combina les paraules "veu" i "phishing". En aquesta tècnica, els atacants utilitzen trucades telefòniques per obtenir informació confidencial de les víctimes. Els delinqüents es fan passar per representants d'entitats confiables, com bancs o institucions governamentals, i demanen informació personal, com números de targetes de crèdit o contrasenyes. Utilitzen tàctiques d'enginyeria social i engany per convèncer les víctimes que divulguin dades sensibles.

El carding, per la seva banda, és una activitat il·legal que involucra l'ús fraudulent de targetes de crèdit i dèbit. Els carders, com se'ls coneix als delinqüents que practiquen el carding, obtenen informació de targetes de crèdit robades o falsificades i realitzen compres en línia o retirs d'efectiu. Utilitzen tècniques com l'skimming (captura de dades de targetes en caixers automàtics) o la compra d'informació de targetes en mercats clandestins a la web fosca.

Per protegir-nos d'aquestes amenaces, és important seguir algunes pautes de seguretat. En primer lloc, hem d'estar atents als missatges de text o trucades telefòniques no sol·licitades. Si reps un missatge que sembla sospitós o una trucada que demana informació personal, no proporcions dades confidencials. En lloc d'això, comunica't directament amb l'entitat en qüestió utilitzant els canals de contacte oficials per verificar l'autenticitat de la sol·licitud.

A més, és fonamental mantenir les nostres aplicacions i sistemes operatius actualitzats. Les actualitzacions sovint contenen la seguretat que tanquen les vulnerabilitats que els atacants poden aprofitar. També és essencial utilitzar soluciones de seguretat confiables, com antivirus i firewalls(tallafocs), per protegir els nostres dispositius contra malware i atacs cibernètics.

L'educació i la consciència són claus en la protecció contra aquestes amenaces emergents. És important informar-se sobre les tàctiques utilitzades pels ciberdelinqüents

6. Decàleg de bones pràctiques per part de l´usuari

- Mantenir la informació personal segura: No comparteixis dades confidencials per correu electrònic, missatges o trucades no sol·licitades. Les entitats legítimes mai et demanaran informació personal per aquests mitjans.

- Verifica l'autenticitat del lloc web: Abans d'ingressar les teves dades en un lloc web , assegura't que la URL sigui correcta i segura (https://) (tot i que a vegades els ciberdelinqüents ja utilitzen el protocol https). Evita fer clic en enllaços enviats per correu electrònic o missatges sospitosos.

- Utilitza contrasenyes segures: Crea contrasenyes úniques per a cada compte o xarxa i assegura't que siguin robustes, utilitzant una combinació de lletres, números i caràcters especials. No utilitzes informació personal predictible.

- Activa l'autenticació de dos factors (2FA): Aprofita l'opció de 2FA per agregar una capa addicional de seguretat als teus comptes o xarxes socials. Això requerirà un segon pas de verificació a més de la teva contrasenya.

- Mantenir els teus dispositius actualitzats: Actualitza regularment el sistema operatiu i les aplicacions dels teus dispositius, ja que les actualitzacions solen incloure millores de seguretat que et protegiran de les amenaces més recents.

- Utilitza una solució de seguretat confiable: Instal·la un programari antivirus confiable i mantén-lo actualitzat per protegir-te de malware i atacs de phishing.

- Tenir cura dels arxius adjunts i els enllaços: No descarreguis arxius adjunts ni facis clic en enllaços sospitosos. Els atacants poden utilitzar aquests mètodes per infectar el teu dispositiu amb malware o redirigir-te a llocs web fraudulents.

- Verifica els correus electrònics sospitosos: Si reps un correu electrònic que sembla provenir d´una entitat però et resulta sospitós, no facis clic en cap enllaç ni descarregues arxius adjunts. Al seu lloc, comunica't directament amb el l´interlocutor per confirmar la legitimitat del correu.

- Mantenir les teves dades personals en privat: Evita realitzar transaccions financeres en xarxes Wi-Fi públiques o no segures. Utilitza una connexió VPN (xarxa privada virtual) per assegurar les teves comunicacions i protegir les teves dades.

- Educar els empleats i clients: Les empreses han de brindar capacitació sobre ciberseguretat als seus empleats i educar els clients sobre les millors pràctiques per protegir-se del phishing. La consciència i l'educació són fonamentals per prevenir atacs reeixits.

7. Mesures de protecció per l´entitat

- Solucions de filtratge de correu electrònic: Implementar solucions de filtratge de correu electrònic que utilitzin tècniques avançades per detectar i bloquejar correus electrònics de phishing. Aquestes solucions poden analitzar el contingut, els enllaços i els adjunts dels correus electrònics a la recerca de senyals de phishing i marcar-los o bloquejar-los.

- Autenticació de correu electrònic: Implementar l'autenticació de correu electrònic, com l'SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) i DMARC (Domain-based Message Authentication, Reporting, and Conformance). Aquestes mesures ajuden a verificar l' autenticitat del remitent i reduir la suplantació d' identitat.

- Capacitat de detecció d' enllaços maliciosos: Utilitzar eines i serveis de detecció d' enllaços maliciosos en els correus electrònics entrants. Aquestes eines poden analitzar els enllaços a la recerca d'URLs sospitoses i advertir els usuaris sobre possibles amenaces.

- Actualitzacions i pegats de seguretat: Mantenir actualitzats els sistemes operatius i les aplicacions utilitzades en la infraestructura crítica. Les actualitzacions i els pegats de seguretat solen incloure correccions per a vulnerabilitats conegudes que podrien ser explotades pels atacants de phishing.

- Firewall i solucions de seguretat de xarxa: Implementar firewalls i solucions de seguretat de xarxa per monitorar i filtrar el trànsit entrant i sortint. Aquestes solucions poden ajudar a detectar i bloquejar intents de phishing abans que arribin als usuaris.

- Conscienciació i capacitació del personal: Proporcionar capacitació i conscienciació regular als empleats sobre les tècniques de phishing i com identificar correus electrònics sospitosos. Això inclou educar-los sobre la importància de no fer clic en enllaços desconeguts, no obrir arxius adjunts sospitosos i no proporcionar informació confidencial a través de correus electrònics.

- Seguretat en navegadors web: Configurar els navegadors utilitzats en la infraestructura crítica per bloquejar o advertir sobre llocs web sospitosos o maliciosos. Això es pot aconseguir a través de la configuració de polítiques de seguretat o mitjançant la instal·lació d'extensions de seguretat.

- Monitoratge i registre d' esdeveniments: Implementar sistemes de monitoratge i registre d' esdeveniments que permetin detectar activitats sospitoses, com intents de phishing o accessos no autoritzats. Això pot ajudar a identificar ràpidament incidents de seguretat i prendre mesures correctives.

- Filtratge de missatges de text: Utilitzar solucions de filtratge de missatges de text que analitzin i bloquegin missatges de text sospitosos o maliciosos. Aquestes solucions poden detectar patrons i contingut associats amb l'smishing i bloquejar els missatges abans que arribin al dispositiu.

- Autenticació de missatges de text: Implementar tècniques d' autenticació de missatges de text, com SenderID, per verificar l' autenticitat del remitent i reduir la suplantació d' identitat.

- Recopilació i anàlisi de registres: Configurar sistemes de registre i esdeveniments en tota la infraestructura per recopilar informació detallada sobre activitats i esdeveniments. Aquests registres poden incloure registres d' accés, registres de firewall, registres de servidor web, registres de sistemes de detecció d' intrusions, entre d' altres. Posteriorment, s' han d' analitzar aquests registres a la recerca de patrons, anomalies i signes d' activitat sospitosa.

- Configuració de sistemes d' alerta primerenca: Configurar sistemes d' alerta primerenca que monitorin els registres i generin alertes en temps real quan es detectin indicadors de compromís coneguts o comportaments anòmals. Aquestes alertes poden enviar-se als equips de seguretat per a la seva investigació i resposta.

- Implementació de sistemes de detecció d'amenaces: Implementar sistemes de detecció d'amenaces avançats, com sistemes de prevenció d'intrusions (IPS), sistemes de detecció d'intrusions (IDS), sistemes d'anàlisi de comportament d'usuari (UBA) o sistemes d'anàlisi de seguretat (SIEM). Aquestes solucions poden detectar i alertar sobre patrons i comportaments sospitosos, així com ajudar en la correlació d'esdeveniments i la generació d'informes detallats.

- Actualització i compartició d'indicadors de compromís: Mantenir actualitzada una llista d'indicadors de compromís (IOC) coneguts, com adreces IP malicioses, URL, hashes d'arxius i patrons de trànsit associats amb amenaces conegudes. Aquests IOC es poden utilitzar per comparar amb els esdeveniments i registres de la infraestructura i detectar possibles amenaces.

- Anàlisi de malware i sandboxing: Utilitzar solucions d' anàlisi de malware i sandboxing per executar arxius i programes sospitosos en un entorn aïllat i observar el seu comportament. Això ajuda a identificar possibles indicadors de compromís i determinar si un arxiu o programa és maliciós.

- Monitoratge i anàlisi de trànsit de xarxa: Configurar solucions de monitoratge i anàlisi de trànsit de xarxa per detectar patrons de trànsit sospitós o comportaments anòmals. Això pot incloure la detecció d' activitats de comandament i control, comunicacions xifrades no autoritzades o transferència de dades inusual.

- Avaluació i gestió de vulnerabilitats: Realitzar avaluacions regulars de vulnerabilitats en la infraestructura i corregir les debilitats identificades. Les vulnerabilitats no mal configurades poden ser aprofitades pels atacants i poden generar indicadors de compromís.

És important destacar que aquestes mesures tècniques s' han de complementar amb mesures organitzatives i de conscienciació, així com amb una resposta efectiva a incidents de seguretat. La protecció contra el phishing és un esforç continu i requerirà una combinació de tecnologia, capacitació i vigilància constant.

8. Auditoria interna de Ciberseguretat

- Definició de l' abast: En primer lloc, s' ha de definir l' abast de l' auditoria, determinant els sistemes, xarxes i actius que seran avaluats. Això inclou identificar les àrees crítiques de l' organització i els actius d' informació sensibles.

- Revisió de polítiques i procediments: Es revisen les polítiques i procediments de seguretat existents per assegurar-se que estiguin actualitzats i alineats amb les millors pràctiques i les regulacions de seguretat aplicables. Això inclou polítiques d' accés, ús acceptable de recursos, gestió de contrasenyes, xifrat de dades, entre d' altres.

- Avaluació de la infraestructura de seguretat: Es duu a terme una revisió de la infraestructura de seguretat existent, incloent firewalls, sistemes de detecció i prevenció d'intrusions (IDS/IPS), sistemes de gestió d'esdeveniments i informació de seguretat (SIEM), antivirus i solucions de protecció d'endpoints.

- Anàlisi de vulnerabilitats i proves de penetració: Es realitzen anàlisis de vulnerabilitats i proves de penetració per identificar possibles bretxes de seguretat en els sistemes i xarxes de l' organització. Aquestes proves ajuden a identificar vulnerabilitats conegudes i avaluar l'efectivitat de les mesures de seguretat implementades.

- Revisió de gestió d' incidents: Es revisa el procés de gestió d' incidents per assegurar-se que estigui correctament establert i documentat. Això inclou la identificació, resposta, notificació i recuperació d' incidents de seguretat, així com el seguiment i anàlisi de lliçons apreses.

- Avaluació del compliment normatiu: Es verifica si l'organització compleix amb les regulacions i normatives de seguretat rellevants

- Avaluació de la conscienciació en seguretat: S' avalua el nivell de conscienciació en seguretat dels empleats de l' organització. Això pot incloure la revisió de programes de formació en seguretat, simulacions de phishing i altres mesures destinades a fomentar una cultura de seguretat.

- Informe i recomanacions: Es prepara un informe detallat que inclou les troballes, les vulnerabilitats identificades i les recomanacions per millorar la seguretat de l' organització. L'informe es presenta a la direcció i es discuteix per assegurar que es prenguin les mesures adequades per abordar les troballes.

9. Pla de resposta a incidents

Un pla de resposta a incidents de ciberseguretat és un document que descriu els procediments i accions a seguir en cas d'un incident de seguretat. A continuació, es presenten les parts clau que solen incloure's en un pla de resposta a incidents de ciberseguretat:

- Introducció: Aquesta secció proporciona una visió general del pla de resposta a incidents, incloent-hi el seu propòsit, abast i objectius. També es poden incloure les responsabilitats i rols dels membres de l' equip de resposta a incidents.

- Definicions: Aquí es proporcionen definicions clares dels termes i conceptes clau utilitzats en el pla. Això assegura una comprensió comuna i precisa entre els membres de l' equip de resposta a incidents i altres interessats.

- Procediments de notificació i activació: Aquesta part descriu els procediments per notificar i activar el pla de resposta a incidents quan es detecta un incident de seguretat. Inclou la identificació dels punts de contacte, les formes de comunicació i les responsabilitats de cada persona involucrada en el procés de notificació i activació.

- Avaluació i classificació d' incidents: En aquesta secció, s' estableixen els criteris per avaluar i classificar els incidents de seguretat. Pot incloure una matriu d' impacte i probabilitat per determinar la gravetat i el nivell de resposta requerit per a cada incident.

- Contenció i mitigació: Aquí es detallen les accions a prendre per contenir i mitigar l' incident de seguretat. Això pot incloure la desconnexió de sistemes afectats, l'aïllament de xarxes, l'aplicació de la seguretat, la restauració de còpies de seguretat, entre altres mesures.

- Investigació i anàlisi d' incidents: Aquesta part descriu els procediments i eines per investigar i analitzar l' incident de seguretat. S' inclouen tècniques de recopilació d' evidència, registre d' activitats, anàlisi forense i seguiment d' incidents.

- Comunicació i coordinació: Aquí s' estableixen els canals de comunicació interns i externs, així com els protocols de coordinació amb les parts interessades, com l' equip de gestió, els departaments legals, les autoritats i els proveïdors de serveis de seguretat.

- Notificació i divulgació: En aquesta secció, es descriuen els procediments per a la notificació i divulgació de l' incident a les parts pertinents, com clients, proveïdors, socis comercials i autoritats reguladores, en compliment de les obligacions legals i de compliment normatiu.

- Restauració i recuperació: Es detallen les mesures i accions necessàries per a la restauració i recuperació dels sistemes i dades afectats per l' incident. Això inclou la implementació de plans de continuïtat del negoci i la revisió de les mesures de seguretat existents.

- Avaluació post-incident i lliçons apreses: Aquesta part del pla se centra en l' avaluació i revisió de l' incident un cop ha estat resolt. S' analitzen les lliçons apreses, s' identifiquen les millores necessàries i s' actualitza el pla de resposta a incidents en base a les troballes.

És important tenir en compte que l' estructura i els elements d' un pla de resposta a incidents poden variar segons l' organització i els seus requisits específics.

10. Glossari de termes

DKIM:(DomainKeys Identified Mail): DKIM és un mètode d'autenticació de correu electrònic que permet verificar l'autenticitat del remitent d'un missatge. S' utilitza una signatura digital basada en claus criptogràfiques per verificar que el contingut del correu electrònic no ha estat modificat i que el remitent és legítim.

DMARC:(Domain-based Message Authentication, Reporting, and Conformance): DMARC és un estàndard d'autenticació de correu electrònic que combina l'autenticació DKIM i SPF per protegir contra el correu electrònic falsificat i el phishing. DMARC permet als remitents especificar com els servidors de correu han de manejar els missatges no autenticats i proporciona informes de compliment i activitat.
Endpoint: Un endpoint es refereix a un dispositiu final, com un ordinador d'escriptori, una laptop, un telèfon mòbil o una tauleta, que s'utilitza per accedir a una xarxa o sistema.

Hash: En criptografia, un hash és el resultat d'aplicar una funció hash a un conjunt de dades, produint una cadena de caràcters de longitud fixa. Els hash s'utilitzen per verificar la integritat de les dades i també s'utilitzen en diversos algoritmes criptogràfics.

IDS: L'IDS (Intrusion Detection System) és un sistema de detecció d'intrusions que monitora i analitza el trànsit de xarxa a la recerca d'activitats i comportaments sospitosos o maliciosos. Identifica possibles intrusions i genera alertes per a la seva posterior anàlisi i resposta.

Malware: És un terme general que engloba tota mena de programari maliciós dissenyat per danyar, infectar o accedir de manera no autoritzada a un sistema informàtic.

Ransomware: És un tipus de malware que xifra els arxius d'un sistema i exigeix un rescat, generalment en criptomonedes, a canvi de la clau de desxifrat.

Phishing: És una tècnica d'enginyeria social utilitzada per obtenir informació confidencial, com contrasenyes o dades sensibles, mitjançant l'enviament de missatges fraudulents que es fan passar per entitats legítimes.

Sandboxing: El sandboxing és una tècnica de seguretat que consisteix a executar aplicacions o processos en un entorn aïllat i controlat, anomenat "sandbox". L' objectiu principal del sandboxing és limitar l' impacte de les aplicacions malicioses o potencialment perilloses en restringir el seu accés a recursos del sistema i dades sensibles.

SIEM: El SIEM (Security Information and Event Management) és una solució de seguretat que recopila, correlaciona i analitza informació d'esdeveniments i registres de diferents fonts en una organització. Permet una visibilitat integral dels esdeveniments de seguretat, la qual cosa facilita la detecció i resposta a incidents. També ajuda en la generació d' informes de compliment normatiu.

Smishing: És una combinació de "SMS" i "phishing". Es refereix a la tècnica d' enviar missatges de text fraudulents per enganyar les víctimes i obtenir informació confidencial.

Skimming: És una tècnica utilitzada per capturar informació de targetes de crèdit o dèbit. Els delinqüents instal·len dispositius il·legals en caixers automàtics o punts de venda per registrar les dades de les targetes i després utilitzar-les per a finalitats fraudulentes.

SOC: s' encarrega de monitorar, detectar, analitzar i respondre a incidents de seguretat en temps real. És responsable de supervisar la infraestructura de TI i els actius d' una organització per garantir la protecció contra amenaces i atacs cibernètics.

SPF:(Sender Policy Framework): SPF és un mecanisme d'autenticació de correu electrònic que permet verificar si el servidor de correu electrònic que envia un missatge està autoritzat per enviar en nom del domini del remitent. S' utilitza un registre SPF en el DNS per especificar els servidors de correu electrònic autoritzats per enviar correus des d' un domini específic.

Vishing: És una combinació de "veu" i "phishing". En aquesta tècnica, els atacants utilitzen trucades telefòniques per obtenir informació confidencial de les víctimes, fent-se passar per entitats legítimes.

Carding: És una activitat il·legal que involucra l'ús fraudulent de targetes de crèdit i dèbit. Els carders obtenen informació de targetes robades o falsificades i la utilitzen per realitzar compres o retirs d' efectiu.

Firewall: És una mesura de seguretat que actua com una barrera entre una xarxa interna i una xarxa externa, controlant el trànsit de dades i filtrant les connexions no autoritzades.

Aquests termes són fonamentals per entendre les amenaces i les mesures de seguretat en l' àmbit de la informàtica i la protecció de dades.