La infecció de dispositius mòbils i l'enviament d'SMS fraudulents: una amenaça creixent

Introducció

La Llei 22/2022, de 9 de juny, encomana a l´Agència Nacional de Ciberseguretat d´Andorra (ANC-AD) l'exercici de les funcions relatives a la seguretat de les tecnologies de la informació i de protecció de les xarxes d´informació. Alhora, confereix a la secretaria d'Estat de Transformació Digital i Telecomunicacions la responsabilitat de dirigir-la.

A l'era digital actual, els dispositius mòbils s'han convertit en una part integral de les nostres vides. Aquesta dependència també ha donat lloc a noves formes d'atacs cibernètics, entre ells la infecció de dispositius mòbils i l'enviament de missatges de text fraudulents. En aquest document explorem els riscos associats a aquest tipus d'amenaces, les seves implicacions i com protegir-nos, gràcies a la col·laboració en ciberseguretat i l´intercanvi de coneixement d'Andorra Telecom, el Cos de Policia d´Andorra, Andorra Digital i l´Agència Nacional de Ciberseguretat.

1. Antecedents

1.1 La infecció de dispositius i l'enviament d'SMS fraudulents: una amenaça creixent

La infecció de dispositius mòbils:

La infecció de dispositius mòbils es produeix quan un *malware* o programari maliciós s'instal·la en un dispositiu sense el coneixement o consentiment de l'usuari. Això pot ocórrer a través de descàrregues d'aplicacions no confiables, enllaços infectats o fins i tot mitjançant l'explotació de vulnerabilitats en el sistema del dispositiu.

Un cop el *malware* s'instal·la, això pot tenir diverses conseqüències danyoses. Una de les més comunes és l'enviament de missatges de text fraudulents des del dispositiu infectat. Aquests missatges solen contenir enllaços maliciosos o sol·licitar informació personal sensible, com números de targetes de crèdit o contrasenyes.

Implicacions dels SMS fraudulents:

L'enviament d'SMS fraudulents pot tenir impactes significatius tant per als individus com per a les organitzacions. Els usuaris poden ser víctimes d'estafes financeres, robatori d'identitat o fins i tot extorsió. A més, el *malware* pot propagar-se a través de la llista de contactes del dispositiu infectat, cosa que significa que amics i familiars també poden veure's afectats.

A l'àmbit empresarial, els SMS fraudulents poden ser utilitzats per al *phishing* - suplantació d'identitat- dirigit a empleats o clients, de la qual cosa poden resultar bretxes de seguretat, pèrdua de dades confidencials i danys a la reputació de l'empresa, a més de processos legals i costos financers associats amb la recuperació i mitigació dels danys causats per la infecció.

1.2 Context actual a Andorra: augment del *malware Redline*

En l'àmbit de la ciberseguretat constantment sorgeixen noves amenaces i formes d'atacs. Una de les més recents i preocupants és coneguda com a *Redline.* En aquest article, expliquem què és, com pot infectar el dispositiu, així com mesures de protecció.

Què és *Redline*?

Redline és una forma de *malware* avançat que s'enfoca principalment a dispositius mòbils. Es classifica com un 'troià bancari', cosa que significa que està dissenyat per prendre informació financera i dades sensibles dels usuaris, especialment a través d'aplicacions bancàries o de pagaments.

La infecció de *Redline* generalment passa quan un usuari descarrega una aplicació maliciosa des de fonts no confiables fora de les botigues *on-line* oficials. Aquestes poden presentar-se com a versions falsificades d'aplicacions populars o com a aplicacions completament noves que prometen oferir beneficis o funcionalitats atractives.

Una vegada que l'usuari instal·la l'aplicació infectada, *Redline* s'activa i comença a executar les seves operacions malicioses en segon pla sense el coneixement de l'usuari.

Com *Redline* pot infectar un dispositiu?

Descàrregues des de fonts no confiables: en descarregar aplicacions de botigues de tercers o llocs web no verificats, augmenta el risc d'infectar-se amb *Redline*. Aquestes fonts solen allotjar versions falsificades o modificades d'aplicacions populars, com per exemple de banca *on-line*, que contenen el *malware*.

Missatges de *phishing*: els ciberdelinqüents poden enviar missatges de *phishing* que contenen enllaços maliciosos a través de SMS, correus electrònics o altres plataformes de missatgeria. En fer clic en aquests enllaços es pot redirigir l'usuari a llocs web falsos o instal·lar directament *Redline* en el dispositiu.

Vulnerabilitats del sistema operatiu: algunes variants de *Redline* poden aprofitar les vulnerabilitats del sistema operatiu per infiltrar-se en el dispositiu sense necessitat d'interacció directa de l'usuari. És fonamental mantenir el sistema operatiu actualitzat per protegir-se contra aquest tipus d'atacs.

2. Frau per mitjà d'SMS a Andorra

Andorra Telecom constata en els darrers mesos un augment de reclamacions relacionades amb l'enviament d'SMS de forma no voluntària per part del client. L'anàlisi de dites reclamacions ha permès l'operadora identificar les principals i fins avui poc freqüents destinacions d'aquests SMS, en països com ara Suècia, Sèrbia i Regne Unit entre d'altres.

Des de la companyia assenyalen que la forma més efectiva per saber si un dispositiu està afectat consisteix en revisar el detall de comunicacions disponible a través de l'aplicació mòbil d'Andorra Telecom o també accedint a l'espai client del portal https://www.andorratelecom.ad/consums.

3. Bones pràctiques

- Descarrega aplicacions només de fonts confiables: utilitza les botigues oficials, com Google Play Store o App Store, per descarregar aplicacions en el teu *smartphone*. Evita descarregar-ne de fonts no verificades o llocs web desconeguts, i vigila amb els permisos que dones a les apps.

- Mantén el teu sistema operatiu actualitzat: les actualitzacions solen incloure la seguretat que protegeix el teu *smartphone* contra vulnerabilitats conegudes. Un programari actualitzat assegura més protecció contra amenaces de *malware*.

- Instal·la un programari antivirus confiable: utilitza una aplicació antivirus coneguda per al teu smartphone. Aquestes aplicacions poden escanejar i detectar *malware*, així com proporcionar funcions de protecció en temps real.

- Sigues cautelós amb els enllaços i missatges desconeguts: evita fer clic en enllaços sospitosos rebuts a través de missatges de text, correus electrònics o aplicacions de missatgeria. No obris missatges o arxius adjunts de remitents desconeguts, ja que podrien contenir *malware*.

- No *rootejar* o fer *jailbreak* al teu dispositiu, és a dir, eliminar restriccions del sistema operatiu o modificar-lo: mantén el teu *smartphone* amb la seva configuració original i evita realitzar processos de *root* o *jailbreak*, ja que això pot comprometre la seguretat del dispositiu i obrir-lo a amenaces de *malware*.

- Configura bloquejos de pantalla segurs: protegeix el teu dispositiu mòbil amb un patró, PIN o identificació biomètrica segura (empremta dactilar o reconeixement facial). Això ajudarà a prevenir l'accés no autoritzat en cas de pèrdua o robatori.

- Activa l'autenticació de dos factors (2FA): habilita l'autenticació de dos factors en les aplicacions i serveis que l'ofereixen. Això proporciona una capa addicional de seguretat en requerir un segon factor de verificació, com un codi enviat al teu *smartphone*, per accedir al teu compte.

- No facilitis codis de seguretat, ni cap dada personal ni confidencial, a ningú.

- Verifica el consum d'SMS de manera periòdica per detectar si hi ha algun enviament anòmal o excessiu de missatges.

- Si has estat víctima d'un frau, avisa els teus contactes perquè no obrin cap missatge que pugui ser maliciós.

- No et connectis a xarxes Wi-Fi públiques, especialment aquelles que no requereixen contrasenya o xifrat. Evita-ho, sobretot, si has de consultar comptes teus i dades personals. Aquestes xarxes poden ser utilitzades per ciberdelinqüents per interceptar les teves dades i comprometre la seguretat del teu dispositiu.

- Realitza còpies de seguretat regularment: realitza còpies de seguretat de les teves dades importants, com fotos, contactes i arxius, en un lloc segur. Si el teu *smartphone* s'infecta amb *malware* o es perd, tindràs una còpia de seguretat per restaurar les teves dades.

- Educació i conscienciació: mantén-te informat de les darreres amenaces de *malware* i pràctiques de seguretat. Aprèn a identificar senyals d'advertència i a prendre precaucions en usar el teu *smartphone*. Comparteix aquesta informació amb familiars i amics per ajudar-los a protegir també els seus dispositius.

- Segueix les xarxes socials de l'Agència de Ciberseguretat, la Policia, Andorra Digital i Andorra Telecom per estar informat de les alertes que es van publicant.

- Seguint aquests consells i bones pràctiques, pots reduir significativament el risc d'infecció de *malware* i protegir el teu *smartphone* d'amenaces cibernètiques. Recorda que la seguretat digital és un procés continu, per la qual cosa és important mantenir-se actualitzat i estar atent a possibles riscos.

4. Procés de denúncia a la Policia

Si malgrat el seguiment dels consells descrits a l'apartat anterior ets víctima d'un ciberdelicte caldria que interposessis una denúncia a la Policia. Per realitzar-ho, cal aportar el màxim d'informació possible: la relació d'SMS enviats, a partir de quina data s'han enviat, si la persona afectada recorda haver instal·lat alguna aplicació o si ha entrat en algun enllaç no habitual en aquell període de temps. Qualsevol detall, per molt insignificant que pugui semblar, pot indicar com s'ha pogut infectar el dispositiu i com s'ha desenvolupat el frau.

5. Glossari de termes

- **2FA** (Autenticació de doble factor): mètode de seguretat que requereix dues formes d'autenticació per verificar la identitat d'un usuari. En general, implica una combinació d'alguna cosa que l'usuari sap (contrasenya) i una cosa que l'usuari posseeix (codi enviat a través d'SMS, aplicació d'autenticació, empremta dactilar, etc).

- **Jailbreak**: procés mitjançant el qual s'eliminen les restriccions imposades pel fabricant o el sistema operatiu en un dispositiu iOS (iPhone, iPad) per permetre la instal·lació d'aplicacions no autoritzades i personalitzacions avançades. Això pot exposar el dispositiu a riscos de seguretat i anul·lar la garantia.

- **Malware**: terme general utilitzat per descriure programari maliciós dissenyat per danyar, infectar o comprometre un dispositiu o sistema. Això inclou virus, troians, *ransomware* i *spyware*, entre d'altres.

- **Phishing**: tècnica utilitzada per ciberdelinqüents per obtenir informació personal i confidencial, com contrasenyes, números de targetes de crèdit o dades bancàries, fent-se passar per entitats legítimes a través de correus electrònics, missatges de text, trucades telefòniques o llocs web falsificats.

- **Rootejar**: procés pel qual s'obtenen privilegis d'administrador (conegut com a accés root o superusuari) en dispositius Android per accedir i modificar àrees del sistema operatiu que normalment estan restringides. Això permet realitzar personalitzacions avançades, però també pot exposar el dispositiu a vulnerabilitats de seguretat.

- **SIM** (Mòdul d'Identificació del Subscriptor): targeta petita i intercanviable utilitzada en dispositius mòbils per identificar l'usuari a la xarxa de telefonia

mòbil. Conté informació com el número de telèfon, la identitat del subscriptor i les dades d'autenticació.

- **Smartphone**: Telèfon mòbil amb capacitats avançades que inclou funcions similars a les d'una computadora, com accés a internet, aplicacions, correu electrònic, navegació per GPS o càmera, entre d' altres.

- **SMS** (Short Message Service): servei de missatges curts utilitzat per enviar i rebre missatges de text en dispositius mòbils. Els missatges de text poden contenir informació com notificacions, codis de verificació o missatges promocionals

- **Spyware**: Programari maliciós dissenyat per recopilar informació personal i confidencial d'un dispositiu sense el coneixement o consentiment de l'usuari.