ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

REDLINE, UN PROGRAMARI MALICIÓS QUE CAL VIGILAR

Juny 2024
Document d'ús públic

1. INTRODUCCIÓ I CONTEXTUALITZACIÓ

«Redline» és el nom amb què es coneix un tipus **de programari maliciós troià** de la família dels *stealers* o *infostealers* (lladres d'informació).

Com el seu nom indica, el Redline Stealer el que fa és robar la informació dels usuaris, principalment des dels seus navegadors web, i la seva funció principal és **recollir dades de l'equip infectat** per enviar-les al servidor de comandament i control.

Aquests tipus de programaris maliciosos que tenen com a objectiu robar credencials i dades personals operen sobretot a través d'eines que ofereixen navegadors web com Google Chrome, Microsoft Edge, Safari, etc., i que són els **gestors de contrasenyes**.

Tanmateix, això pot ser una arma de doble tall, ja que aquests gestors de contrasenyes són els més **insegurs del seu gènere**, i el Redline Stealer n'és la millor prova.

Per tant, la seva principal via de transport són els **correus electrònics** i la **publicitat de Google** que podem trobar en els llocs web, encara que també a vegades ha aparegut «camuflat» en forma de **programa d'edició de fotos**.

2. INFECCIÓ PER PART DE L'USUARI

La principal via de distribució de Redline és a través de les **campanyes de pesca**, tot i que també s'ha detectat en **aplicacions de missatgeria modificades** i en **llocs web maliciosos**.

Redline el que fa és **recopilar informació dels navegadors web dels equips dels usuaris**, com, per exemple, les galetes, les claus desades, les dades que emplena l'usuari, informació de les targetes de crèdit, les credencials que s'utilitzen per iniciar sessió a través de la VPN, els registres de xat, etc.

A més a més, aquest programari maliciós també recopila **dades del sistema de la víctima**, com, per exemple, l'adreça IP, el país, la ciutat, el nom de l'usuari, la distribució del teclat, el sistema operatiu, etc.

Com és habitual, hi ha versions de Redline que són molt més modernes i recents i que també s'utilitzen per **robar criptomonedes**. Alguns dels moneders més vulnerables són: Armory, AtomicWallet, BitcoinCore, Bytecoin, etc.

3. FLUX D'ACTUACIÓ PER PART DE REDLINE

1. L'usuari rep un correu electrònic amb un enllaç sospitós/maliciós (pesca).

2. La víctima accedeix al web fraudulent.

3. L'usuari es descarrega l'executable maliciós.

4. La víctima executa el programari maliciós i aquest compromet el sistema.

5. El programari maliciós recopila tota la informació econòmica i financera de l'usuari.

6. Possible fase de postexplotació sota demanda.

4. ÚS I BONES PRÀCTIQUES PER EVITAR SER INFECTATS PER REDLINE

- ✔ *Activa l'**autenticació de doble factor** en tots els comptes que t'ho permetin.*
- ✔ *Cal que tinguis consciència i reforcis, conjuntament amb tots els membres de l'organització professional a la qual pertanys, la importància de **no fer clic a enllaços** que sembli que no són segurs.*
- ✔ *Evita **descarregar-te programari** fora dels llocs dels proveïdors o de les botigues en línia del teu sistema operatiu.*
- ✔ ***No desis contrasenyes o números de targetes de crèdit** al navegador web.*
- ✔ ***Elimina les galetes** amb certa freqüència.*
- ✔ *Implementa sistemes com **DKIM**, **DMARC** i **SPF** al correu electrònic de l'organització.*
- ✔ *Instal·la't un bon **antivirus** i **programari antimalicions** des dels seus propis llocs web o de botigues oficials (com ara Google Play o App Store).*
- ✔ *Gestiona de manera segura les teves **credencials i contrasenyes**.*

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.