



 jdoe@dominio.com



Robos por Malware: Fraudes de datos

Breach Monitoring

de Prey





Los registros de bots proporcionan a los criminales toda la información que necesitan para suplantar a sus usuarios y eludir las medidas antifraude/autenticación:

Datos de inicio de sesión

- ◆ Credenciales
- ◆ Cookies

Datos del dispositivo

- ◆ Huellas del navegador
- ◆ Direcciones IP

Datos personales



APROPIACIÓN DE CUENTAS



IDENTIDADES SINTÉTICAS



FRAUDE SIN TC PRESENTE



ROBO DE IDENTIDAD



FRAUDE DE TRIANGULACIÓN



Cookies: detectando lo indetectable

Cuando un criminal infecta un dispositivo con malware,

los registros de ese dispositivo pueden ayudarles a suplantar al usuario real.



Las cookies pueden permitir a los criminales eludir la MFA o las credenciales. ¡O ambas!



Authentication code

Didn't get a code? [Resend to +X-XXX-XXX-7425](#)

12345678

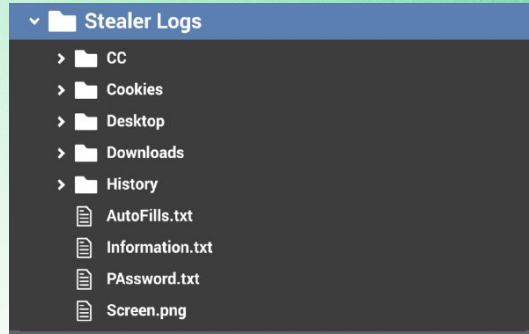
☒ Remember this device (30 days)

Complete login

Muchos sitios usan cookies para recordar "dispositivos confiables" y logran evitar el MFA y/o uso de contraseñas en el siguiente inicio de sesión. Los criminales han estado abusando de esta vulnerabilidad para robar cuentas.



Lo que el criminal ve en los registros de robo

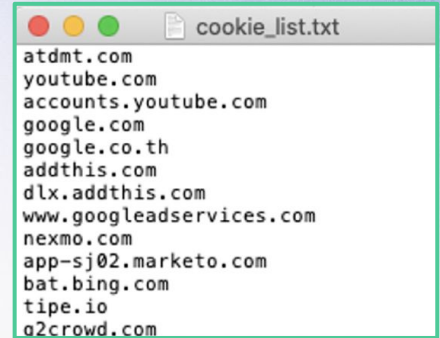
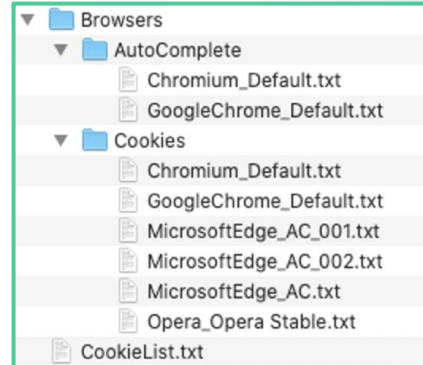
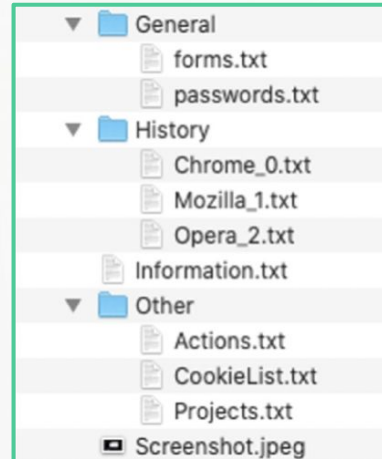


```
MachineID : 2D6A07765DFA3332743865
BIN_PATH : C:\Windows\INF\intelw.PNF

Windows : 10.0 x64 Windows 10 Enterprise
Computer(Uusername) : DESKTOP-D53S7M(Edward)
Screen: 1920x1080
Layouts: en/
LocalTime: 20/7/2021 13:29:16
Zone: UTC+8:0

CPU Model: Intel(R) Core(TM) i7-10710U CPU @ 1.10GHz
CPU Count: 12
GetRAM: 32572
Video Info
Intel(R) UHD Graphics
Intel(R) UHD Graphics
Intel(R) UHD Graphics

[Soft]
Google Chrome(91.0.4472.164)
```





Cómo acceden los criminales a las cookies

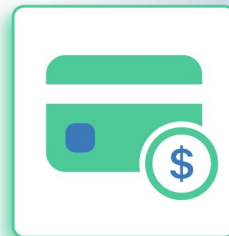
Despliegan malware directamente a los usuarios:

- Adquieren kits o servicios de phishing
- Acceden a servicios de spam
- Alquilan espacio publicitario para malvertising
- Hacen uso de sitios de pago por instalación
- Identifican vulnerabilidades del navegador

Compran en mercados criminales:

Los precios pueden variar de \$3 a *miles de dólares*

Hallan o comercian en foros criminales



Uso indetectable de cookies

Los criminales utilizan navegadores anti-detección para aprovechar las cookies robadas, lo que:

- Permite a los criminales usar las huellas de navegador de usuarios reales
- Proporciona anonimato en la arbitraje de tráfico
- Garantiza confidencialidad completa
- Permite a los criminales trabajar con múltiples cuentas al mismo tiempo en un perfil

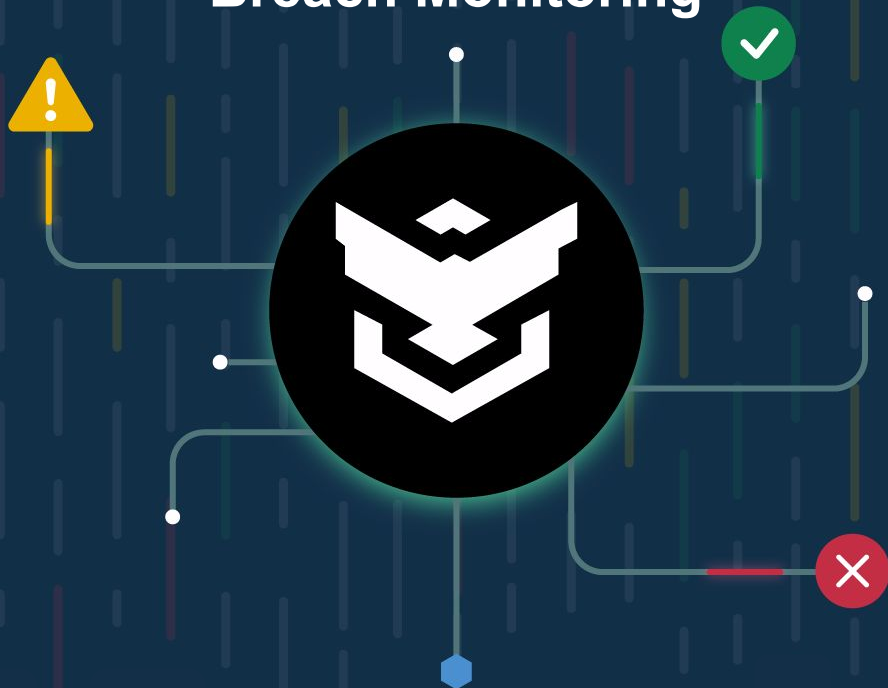


Atención: Cookies





Breach Monitoring



Agenda una Demo en vivo