/Rooted

# EvilnoVNC

## Next-Gen Spear Phishing Attacks

@JoelGMSec

#ROOTED2023
#ROOTEDCON

# Whoami

Joel Gámez Molina // @JoelGMSec

- Security Consultant @ Deloitte - Red Team Operations
- SysAdmin con más de diez años de experiencia
- Ex-CTO de la startup Cyberguard (durante 2 años)
- Profesor de Hacking Ético, Pentesting y PowerShell para organismos y universidades de alto nivel
- Ponente en congresos de ciberseguridad a nivel nacional e internacional (Black Hat USA 20/21, Black Hat EU 22)
- Creador y escritor del blog personal darkbyte.net
- Programador de “hacking tools” (AutoRDPwn, Cloudtopolis, Invoke-DNSteal, PyShell, PSRansom..)

# Prólogo

Uno de los principales vectores de ataque en los ejercicios de Red Team, y posibles puntos de entrada para un atacante, son las campañas de Phishing.

Actualmente, existen todo tipo de herramientas y contramedidas para realizarlas o protegernos contra ellas, con un nivel de madurez muy alto y totalmente consolidadas por la industria de la ciberseguridad.

Por otra parte, apenas existen herramientas orientadas al Spear Phishing o a cualquier otro tipo de ataque más sofisticado, independientemente de si tu objetivo es atacar o defenderte contra ello.

# Historia

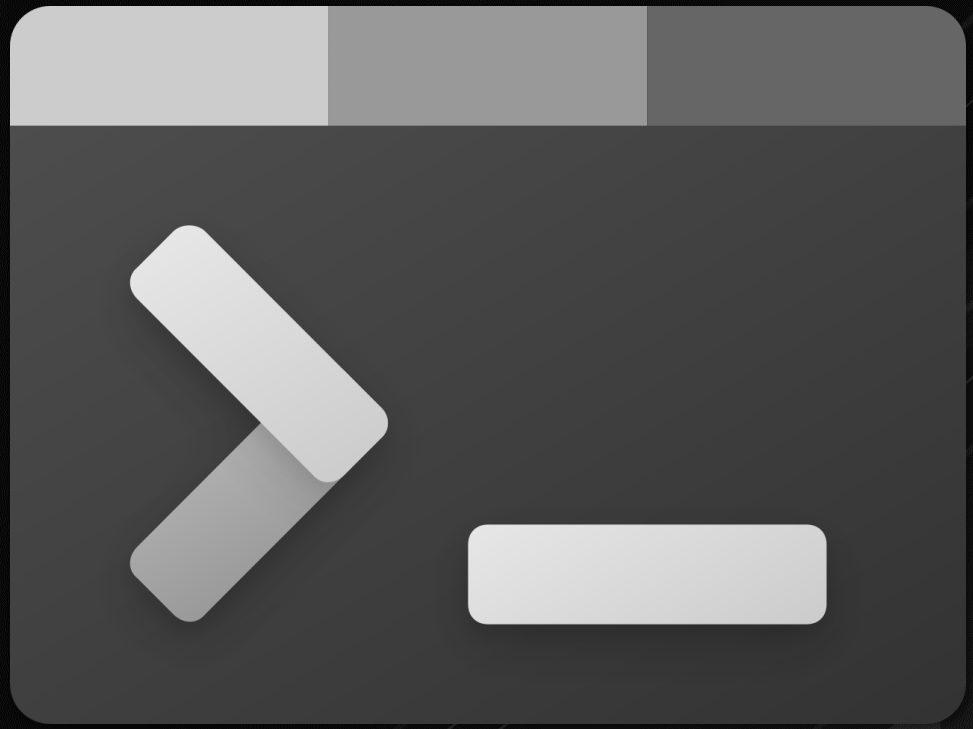
- Un cliente solicita una campaña avanzada de Spear Phishing
- Las pruebas deben incluir la técnica “Browser in the Browser”
- Las víctimas están concienciadas y tienen un nivel avanzado
- Las pruebas deben realizarse sobre la intranet de la compañía
- Todas las medidas de seguridad se encontrarán habilitadas
- Todas las cuentas de usuario están protegidas por 2FA
- Es indispensable conseguir acceso completo con algún usuario

# Episodio I

## Técnicas habituales

# Herramientas

- github.com/UndeadSec/SocialFish
- github.com/rsmusllp/king-phisher
- github.com/drk1wi/Modlishka
- github.com/kgretzky/evilginx2
- github.com/gophish/gophish
- github.com/fin3ss3g0d/evilgophish
- github.com/trustedsec/social-engineer-toolkit



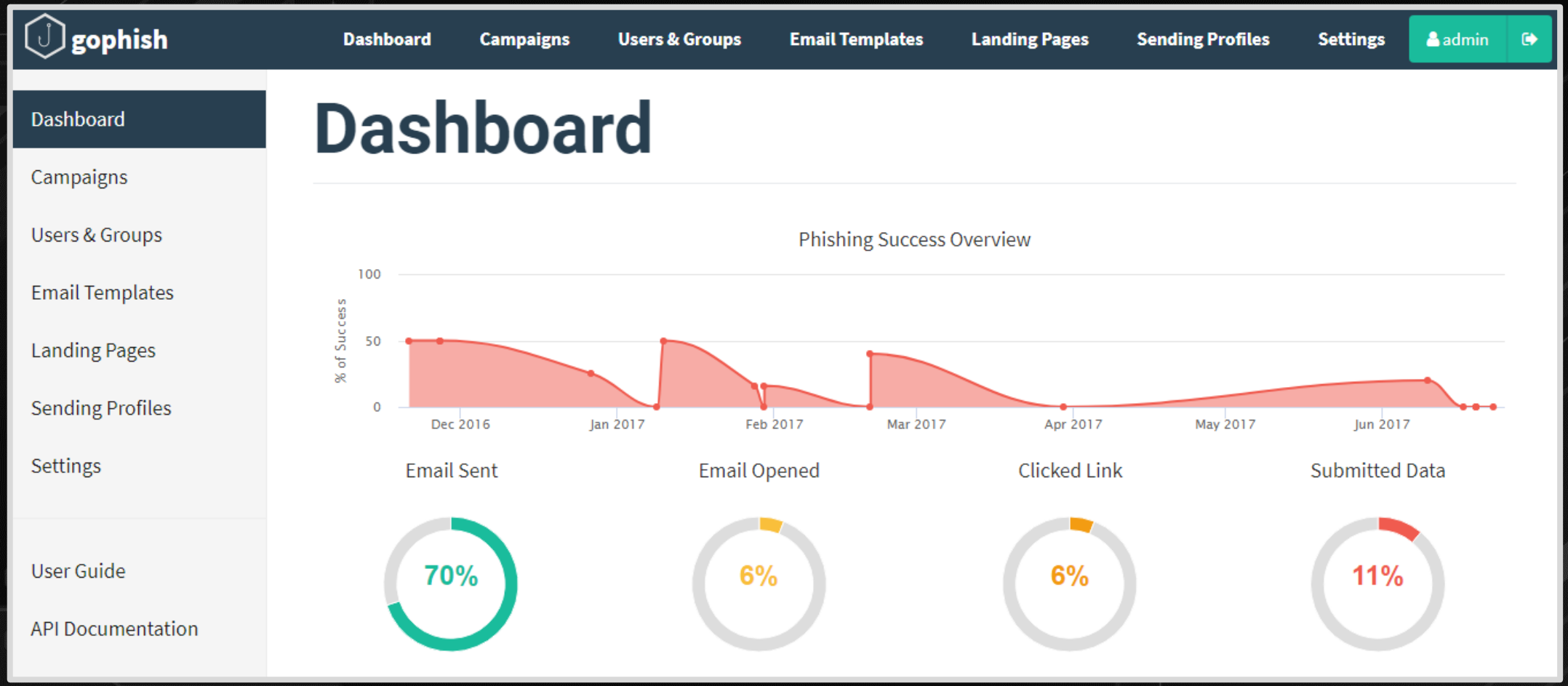
# GoPhish

github.com/gophish/gophish

- No funciona como proxy inverso por defecto
- Es necesario configurar un servidor SMTP
- Se necesitan conocimientos de HTML/CSS
- Acceso y gestión a través de un panel web
- Estadísticas y trazabilidad avanzadas
- Gran nivel de madurez y documentación

# GoPhish

github.com/gophish/gophish



# :) DEMO

Your PC is perfectly stable and is running with absolutely no problems whatsoever.

1000% Complete

For more information about this talk, visit https://github.com/JoelGMSec/EvilnoVNC

You can search for this status code online if you'd like:
Stop code: ALL_SYSTEMS_GO

# Evilginx2

github.com/kgretzky/evilginx2

- Funciona como un Man-in-the-Middle
- No requiere mucha configuración
- Existen multitud de “Phishlets”
- Acceso y gestión a través de consola
- Uso sencillo pero con poca trazabilidad
- Gran nivel de madurez y documentación

# Evilginx2

github.com/kgretzky/evilginx2

```
[14:58:53] [inf] loading phishlets
[14:58:53] [inf] loading configura
[14:58:53] [inf] blacklist mode se
[14:58:53] [inf] redirect paramete
[14:58:53] [inf] verification para
[14:58:53] [inf] verification toke
[14:58:53] [inf] unauthorized requ
[14:58:53] [inf] blacklist: loaded
[14:58:53] [war] server domain not
[14:58:53] [war] server ip not set
```

| phishlet | author | active | status | hostname |
|---|---|---|---|---|
| amazon | @customsync | disabled | available | |
| facebook | @charlesbel | disabled | available | |
| linkedin | @mrgretzky | disabled | available | |
| tiktok | @An0nUD4Y | disabled | available | |
| twitter-mobile | @white_fi | disabled | available | |
| wordpress.org | @meitar | disabled | available | |
| airbnb | @AN0NUD4Y | disabled | available | |
| booking | @Anonymous | disabled | available | |
| github | @audibleblink | disabled | available | |
| paypal | @An0nud4y | disabled | available | |
| protonmail | @jamescullum | disabled | available | |
| twitter | @white_fi | disabled | available | |
| outlook | @mrgretzky | disabled | available | |
| reddit | @customsync | disabled | available | |
| citrix | @424f424f | disabled | available | |
| coinbase | @An0nud4y | disabled | available | |
| instagram | @charlesbel | disabled | available | |
| o365 | @jamescullum | disabled | available | |
| okta | @mikesiegel | disabled | available | |
| onelogin | @perfectlylog... | disabled | available | |

# :) DEMO

Your PC is perfectly stable and is running with absolutely no problems whatsoever.

1000% Complete

For more information about this talk, visit https://github.com/JoelGMSec/EvilnoVNC

You can search for this status code online if you'd like:
Stop code: ALL_SYSTEMS_GO

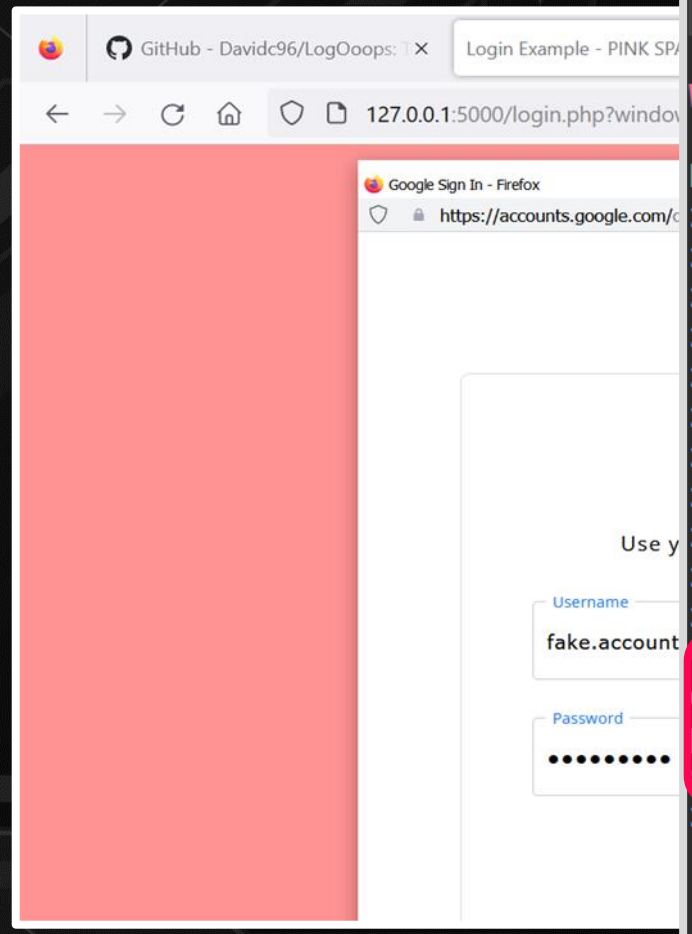
# Episodio II

## Nuevas Técnicas

# Browser in the Browser

- Facilidad de instalación y despliegue
- No requiere mucha configuración
- Se necesitan conocimientos de HTML/CSS
- Acceso y gestión a través de consola
- Compatibilidad con múltiples plataformas
- Poca trazabilidad y poca documentación

# Browser in the Browser




```
✓ JoelGMSec ../Tools/LogOoops master flask run
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
127.0.0.1 - - [02/Mar/2023 17:47:19] "GET /login.php?window_mode=light&language=e
127.0.0.1 - - [02/Mar/2023 17:47:19] "GET /static/css/windows/firefox/light/style
127.0.0.1 - - [02/Mar/2023 17:47:19] "GET /static/css/styles.css HTTP/1.1" 200 -
127.0.0.1 - - [02/Mar/2023 17:47:19] "GET /static/js/windows/firefox/light/script
127.0.0.1 - - [02/Mar/2023 17:47:19] "GET /static/images/logo.png HTTP/1.1" 200 -
127.0.0.1 - - [02/Mar/2023 17:47:19] "GET /static/images/background.jpg HTTP/1.1"
127.0.0.1 - - [02/Mar/2023 17:47:20] "GET /google HTTP/1.1" 200 -
127.0.0.1 - - [02/Mar/2023 17:47:20] "GET /static/images/firefox_logo.svg HTTP/1.
127.0.0.1 - - [02/Mar/2023 17:47:20] "GET /static/images/sec_shield.png HTTP/1.1"
127.0.0.1 - - [02/Mar/2023 17:47:20] "GET /static/js/windows/firefox/light/script
127.0.0.1 - - [02/Mar/2023 17:47:20] "GET /static/images/ssl.svg HTTP/1.1" 200 -
------------- Credentials stolen --------------
email: fake.account@gmail.com
password: Passw0rd!
sign-in: Sign In
127.0.0.1 - - [02/Mar/2023 17:47:26] "POST /credentials HTTP/1.1" 200 -
```

# :) DEMO

Your PC is perfectly stable and is running with absolutely no problems whatsoever.

1000% Complete

For more information about this talk, visit https://github.com/JoelGMSec/EvilnoVNC

You can search for this status code online if you'd like:
Stop code: ALL_SYSTEMS_GO

# Episodio III

## Welcome to the future

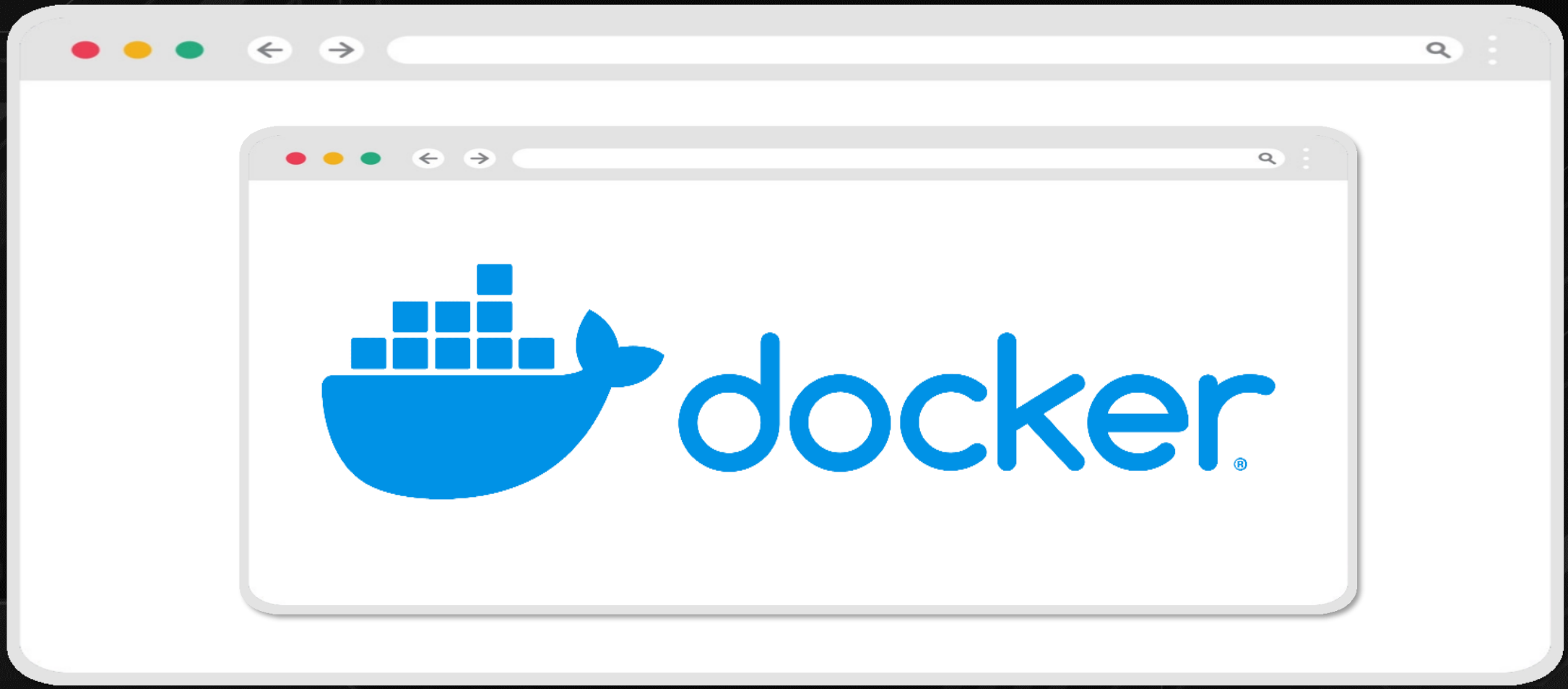
# EvilnoVNC

github.com/JoelGMSec/EvilnoVNC

- Funciona como un Man-in-the-Middle
- No necesita ninguna configuración
- Descifrado de cookies en tiempo real
- Keylogger y visualización en directo
- Interceptación de ficheros automática
- Análisis offline de la navegación

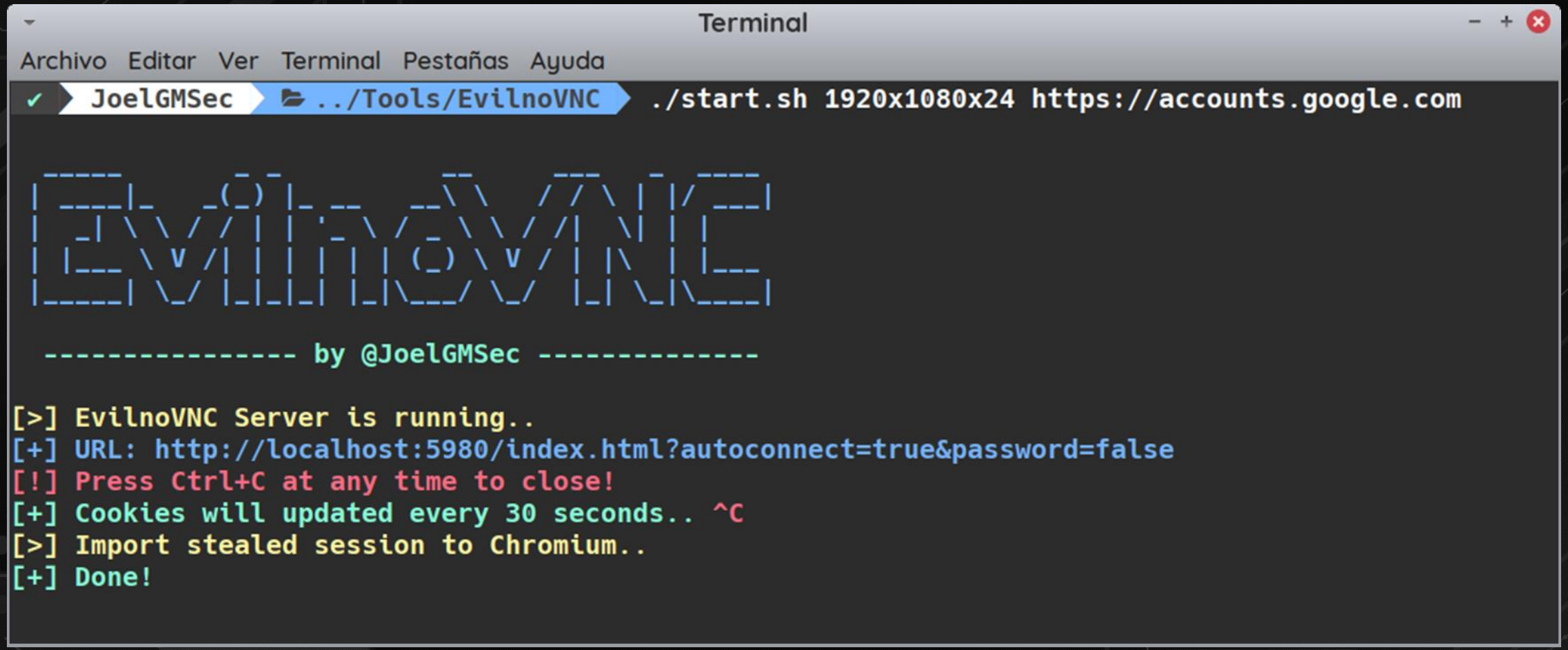
# EvilnoVNC

github.com/JoelGMSec/EvilnoVNC



# EvilnoVNC

github.com/JoelGMSec/EvilnoVNC



# :) DEMO

Your PC is perfectly stable and is running with absolutely no problems whatsoever.

1000% Complete

For more information about this talk, visit https://github.com/JoelGMSec/EvilnoVNC

You can search for this status code online if you'd like:
Stop code: ALL_SYSTEMS_GO

# Episodio IV

## Bonus Stage!

# EvilnoVNC – Multi!

github.com/wanetty/EvilnoVNC

- Idéntico al EvilnoVNC original
- Soporta conexión multi-usuario
- Proxy inverso basado en nginx

.....

- Más complejidad de visualización
- Posible DoS al recibir N peticiones

# :) DEMO

Your PC is perfectly stable and is running with absolutely no problems whatsoever.

1000% Complete

For more information about this talk, visit https://github.com/JoelGMSec/EvilnoVNC

You can search for this status code online if you'd like:
Stop code: ALL_SYSTEMS_GO

# Cosas por hacer

- Compatibilidad con más resoluciones
- Modificar la URL de la víctima con JS
- Replicar el User-Agent original
- Implementación propia de WebSockets
- Diferentes plantillas de carga dinámica
- Crear un gestor de perfiles importados

# Agradecimientos

@mrd0x

@Davidungus

@gm_eduard

@rootedcon

@securiters


# Gracias!

## Preguntas?

@JoelGMSec