EvilnoVNC

Ready to go Phishing Platform

Whoami

Joel Gámez Molina // @JoelGMSec

- Security Consultant @ Deloitte - Red Team Operations
- System adminitrator for more than 10 years
- Ex-CTO of the Cyberguard startup (2 years)
- Professor of Ethical Hacking, Pentesting and PowerShell
- Speaker at national & internacional cibersecurity conferences (Black Hat USA 20/21/23, Black Hat EU 22)
- Creator and writer of the blog darkbyte.net
- Hacking tools programmer (AutoRDPwn, Cloudtopolis, Invoke-DNSteal, PyShell, PSRansom, Thunderstorm..)

Prologue

One of the main attack vectors in Red Team exercises, and possible entry points for an attacker, are phishing campaigns.

Currently, there are all kinds of tools and countermeasures to perform or protect against them, with a very high level of maturity and fully consolidated by the cybersecurity industry.

On the other hand, there are hardly any tools oriented to Spear Phishing or any other type of more sophisticated attack, regardless of whether their purpose is to attack or defend against it.

History

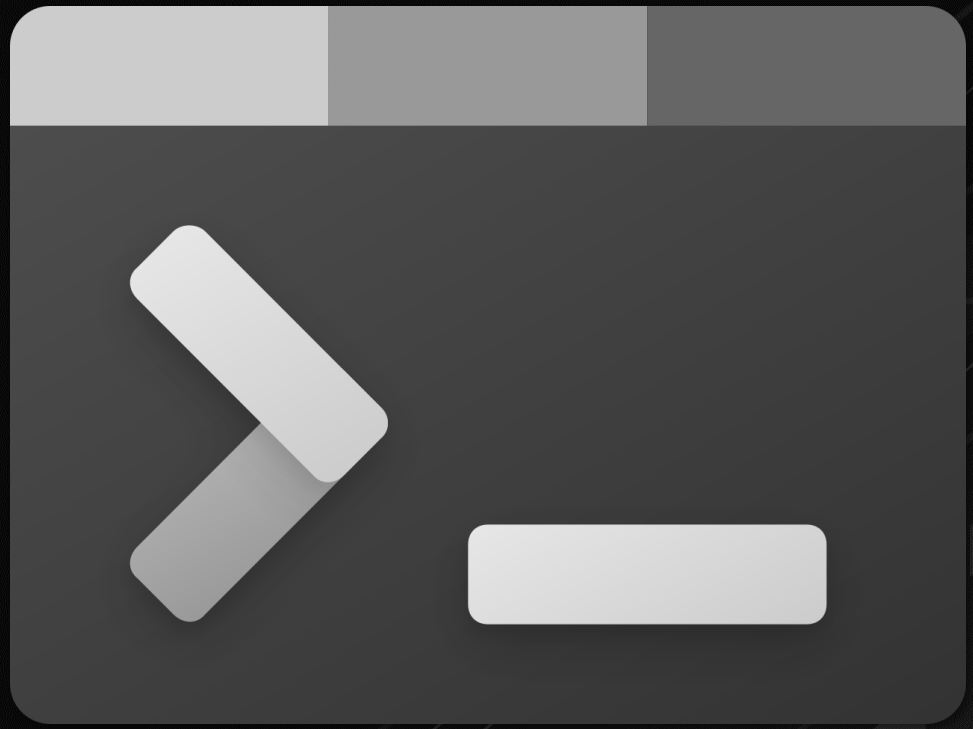
- A customer requests an advanced Spear Phishing campaign
- The tests must include the "Browser in Browser" technique
- The victims are aware and have an advanced level of knowledge
- All security measures must be enabled, like DLP or EDR
- Testing must be performed on the company intranet
- All user accounts must be 2FA protected

Chapter I

Common Techniques

Common Tools

- 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



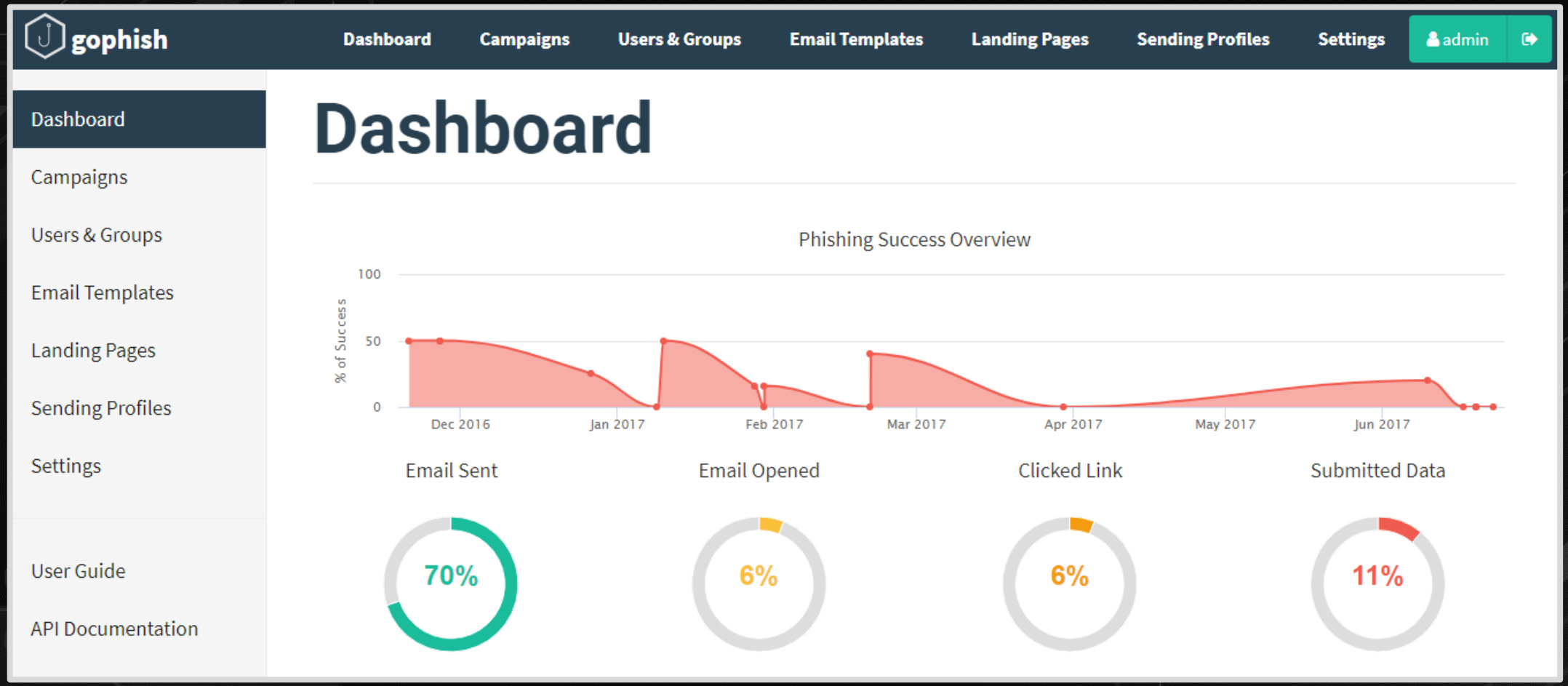
GoPhish

github.com/gophish/gophish

- Doesn't work as a reverse proxy by default
- SMTP server configuration required
- HTML/CSS knowledge required
- Web Access and management
- Advanced statistics and traceability
- High level of maturity and documentation

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

- Works as a Man-in-the-Middle
- Does not require much configuration
- A multitude of "Phishlets" are available
- Console access and management
- Easy to use but with little traceability
- High level of maturity and information

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

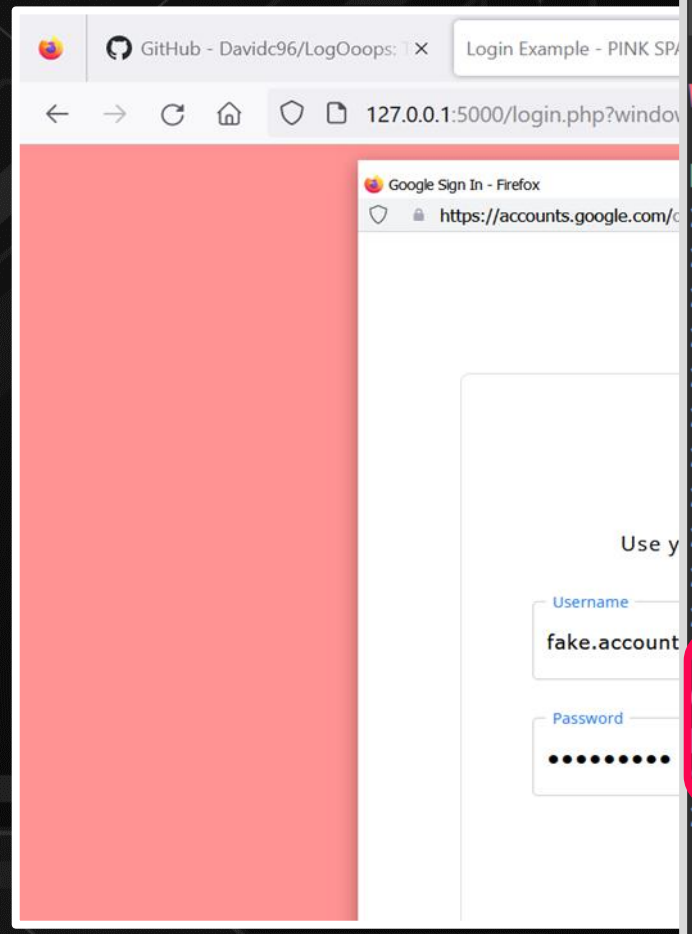
Chapter II

New Techniques

Browser in the Browser

- Ease of installation and deployment
- Does not require a lot of configuration
- HTML/CSS knowledge required
- Console access and management
- Cross-platform compatibility
- Little traceability and documentation

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

Chapter III

Welcome to the future

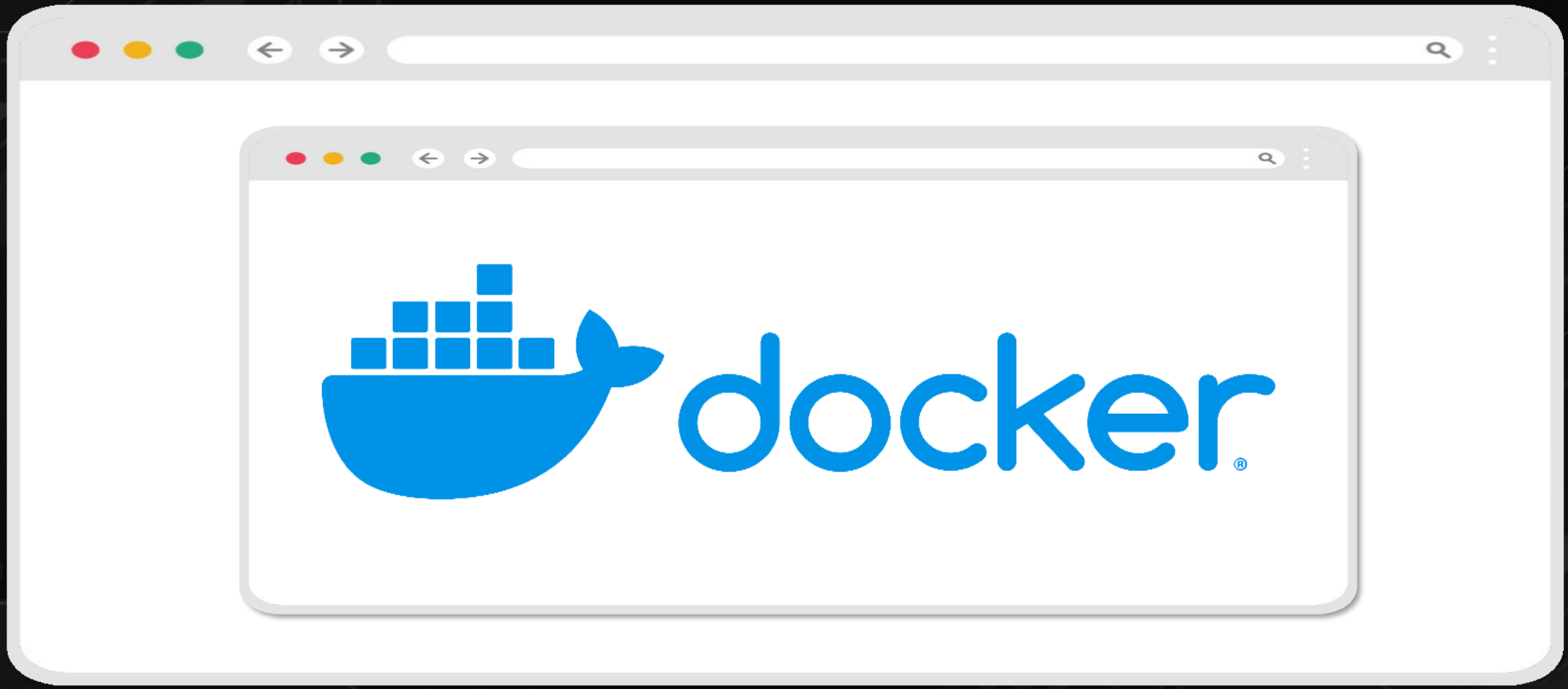
EvilnoVNC

github.com/JoelGMSec/EvilnoVNC

- Works as a Man-in-the-Middle
- No configuration required
- Real-time cookie decryption
- Keylogger and live viewing
- Automatic file interception
- Offline browsing analysis

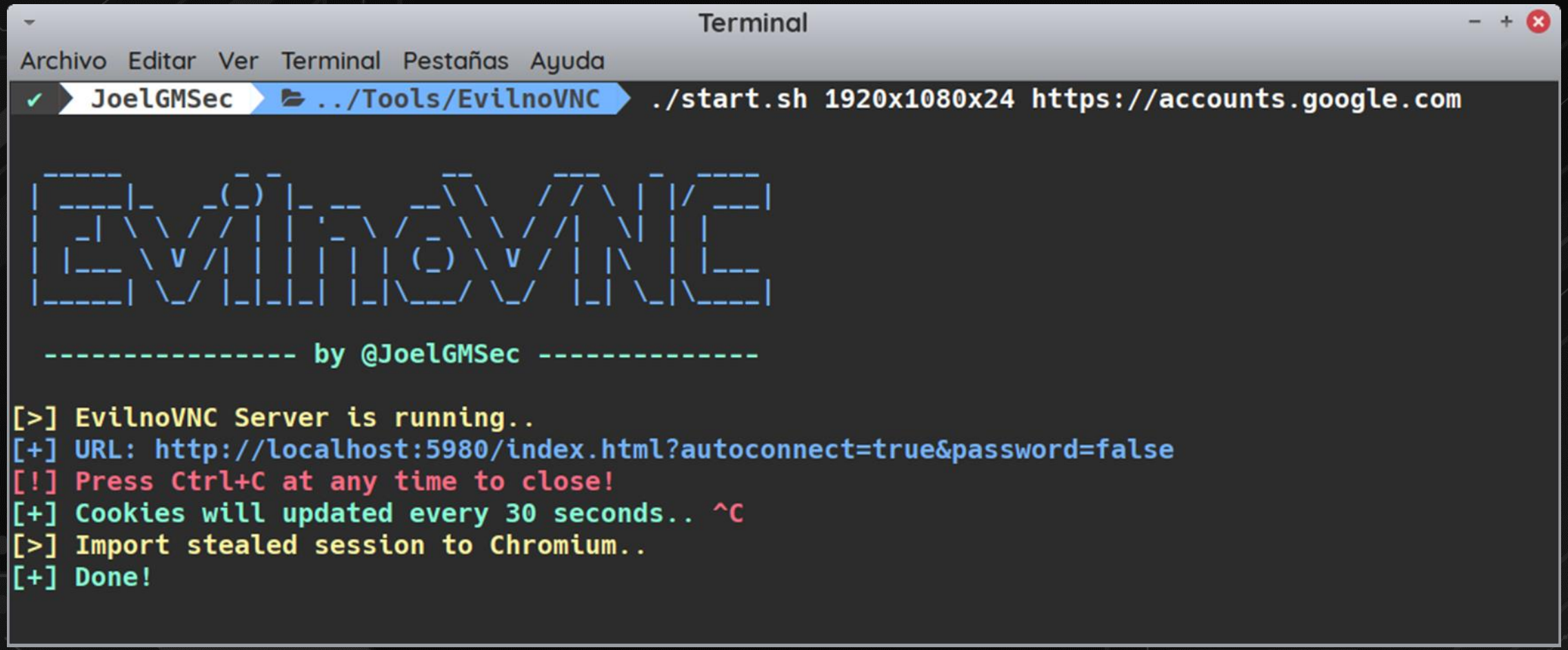
EvilnoVNC

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

Chapter IV

Bonus Stage!

EvilnoVNC – Multi!

github.com/wanetty/EvilnoVNC

- Identical to the original EvilnoVNC
- Multi-user connection support
- Reverse proxy based on nginx
- Profile data sorted in directories
- Higher display complexity
- Possible DoS whit a lot of requests

:) 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

Things To Do

- Support for more resolutions
- Modify victim URL with JS
- Replicate the original User-Agent
- Own implementation of WebSockets
- Different dynamic loading templates
- Create an imported profile manager

Thank you!

Questions?

@JoelGMSec