

# Tácticas & Técnicas de Robos de Identidad

Julio Ureña, PlainText



# net user PlainText

- ❑ Julio Ureña
- ❑ Cristiano / Esposo / Padre / Amigo
- ❑ Líder de la Comunidad RedTeamRD
- ❑ Twitter: @JulioUrena
- ❑ Blog: <https://plaintext.do>
- ❑ YouTube: <https://www.youtube.com/c/JulioUreña>



# Había una vez, un super heroe...



# Contraseñas Robadas

Breaches you were owned in

[https://anonfile.com/M9r6M0v9nb/myfitnesspal\\_rar](https://anonfile.com/M9r6M0v9nb/myfitnesspal_rar)

```
root@plaintext:~/Downloads/myfitnesspal# ls
```

```
file00.txt  file12.txt  file24.txt  file36.txt  file48.txt  file60.txt  
file01.txt  file13.txt  file25.txt  file37.txt  file49.txt  file61.txt  
file02.txt  file14.txt  file26.txt  file38.txt  file50.txt  file62.txt
```

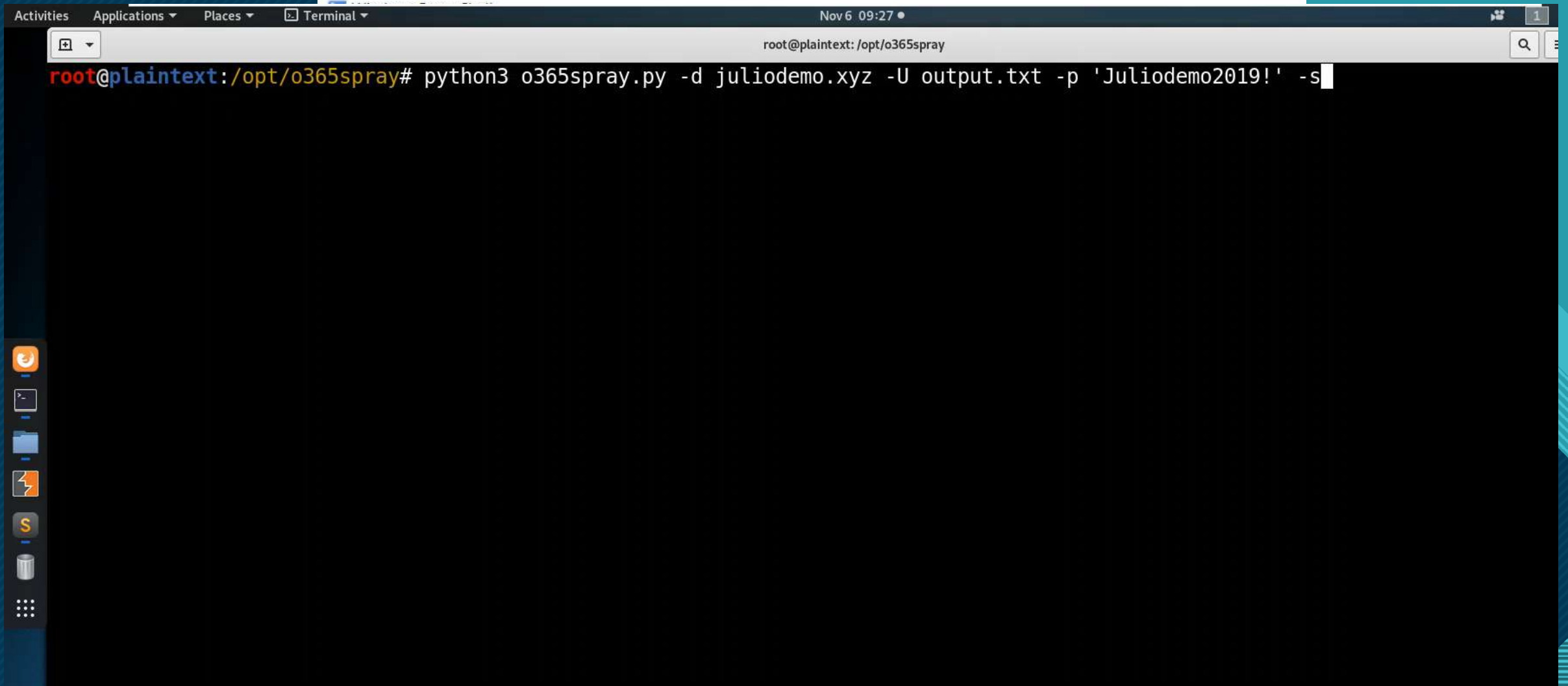
```
root@plaintext:~/Downloads/myfitnesspal# cat file32.txt |grep -v null | head -n 10
```

```
"clmasters70@.com", "tundra"  
"clmasters@.com", "masters4"  
"clmasterson@.com", "celebrate"  
"clmastin@.edu", "classof07"  
"clmastria@.net", "buddy511"  
"clmasullo@gmail.com", "869633"  
"clmat39@.com", "stacey12"  
"clmata82@.com", "shanks3"  
"clmata_2004@.com", "clmata209"  
"clmata1a@.com", "chris1967"
```

known as the "Email Address Leak". It was a breach of a database that contained the names of users back to August that year. The exposed data included usernames, email addresses and weak MD5 hashes of passwords.

**Compromised data:** Email addresses, Passwords, Usernames

# Password Spray

A screenshot of a Linux terminal window. The window title bar shows 'Activities', 'Applications', 'Places', and 'Terminal'. The top status bar indicates 'Nov 6 09:27'. The terminal prompt is 'root@plaintext: /opt/o365spray'. The command being executed is 'python3 o365spray.py -d juliodeemo.xyz -U output.txt -p 'Juliodemo2019!' -s'. The command is partially entered, with a cursor at the end. The terminal background is black, and the text is white. On the left side of the terminal window, there is a vertical dock with several application icons: a terminal icon, a folder icon, a lightning bolt icon, a terminal icon, a terminal icon, and a terminal icon.

```
root@plaintext: /opt/o365spray
root@plaintext:/opt/o365spray# python3 o365spray.py -d juliodeemo.xyz -U output.txt -p 'Juliodemo2019!' -s
```

<https://github.com/byt3bl33d3r/SprayingToolkit>

<https://github.com/zdhsec/o365spray>



# Spear Phishing



# Detalles - Spear Phishing

Necesitamos:

1. Un buen mensaje (Ingeniería Social)
2. Un Dominio (C2 y/o URL)
3. Evadir los controles de seguridad
  - Email Gateways
  - Firewalls
  - Endpoints

# Expired Domain - Spear Phishing

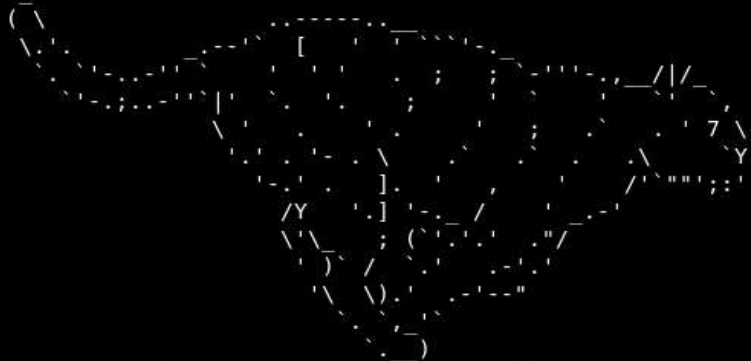
The screenshot shows the ExpiredDomains.net website interface. At the top, there's a navigation bar with 'ExpiredDomains.net', 'Saved Searches', 'Links', 'Plaintext', and a 'Domain Search' input field. Below this, there are tabs for 'Deleted Domains (172)' and 'Marketplace Domains (37)', along with a 'Column Manager' button. A grid of filters is visible, including 'Deleted Domains', 'Deleted .com', 'Deleted .net', 'Deleted .org', 'Deleted .info', 'Deleted .biz', 'ccTLDs A', 'ccTLDs BC', 'ccTLDs DEF', 'ccTLDs G', 'ccTLDs HI', 'ccTLDs JKL', 'ccTLDs MNO', 'ccTLDs PQR', 'ccTLDs S', 'ccTLDs TU', 'ccTLDs VWXYZ', 'gTLDs', 'ngTLDs', 'Caught Domains', 'Pending Delete', and '★ Watchlist'. Below the filters, there's a 'Current Issues (0)' section stating 'At the moment there are no known issues.' and a 'Latest Development' section with RSS feed. The 'Latest Development' section lists several updates from 2019-10-22 to 2019-11-28, including fixes for Epik.com links and new marketplace lists. On the right, there's a 'Domain List Stats & Explanation' table with columns for Name, Update Interval, Time Window, Domains, and New Domains. The table lists various domain categories and their corresponding statistics.

Domain List Stats & Explanation			Deleted Domains	Marketplace Domains
Name	Update Interval	Time Window	Domains	New Domains
Deleted .com Domains	Once Daily	06:00 PM - 10:00 PM *	2,251,732	74,733
Deleted .net Domains	Once Daily	06:00 PM - 10:00 PM *	1,260,080	7,038
Deleted .org Domains	Once Daily	02:30 PM - 03:30 PM *	1,728,304	6,614
Deleted .info Domains	Once Daily	11:30 AM - 12:00 AM *	1,859,109	3,763
Deleted .biz Domains	Once Daily	05:20 PM - 06:00 PM *	829,223	1,200
Deleted .mobi Domains	Once Daily	03:20 AM - 04:30 AM *	797,967	225
Deleted .asia Domains	Once Daily	02:30 AM - 02:50 AM *	323,923	93
Deleted .eu Domains	Once Daily	06:00 PM - 06:15 PM *	529,030	1,102
Deleted .cat Domains	Hourly	Hourly	41,937	70
Deleted .jobs Domains	Hourly	Hourly	1,703	2
Deleted .pro Domains	Once Daily	11:30 AM - 12:00 AM *	274,423	317
Deleted .travel Domains	Hourly	Hourly	3,771	61



# Domain Category - Spear Phishing

```
root@plaintext:/opt/domainCat# python3 domainCat.py --domain newstreamcapital.com
```



```
domainCat - Domain Categorization Discovery at it's finest
written by: l0gan

[*] Targeting Bluecoat WebPulse
[*] Checking category for newstreamcapital.com
[!] Site categorized as: Finance
[*] Targeting Fortiguard
[*] Checking category for newstreamcapital.com
[!] Site categorized as: Finance and Banking
[*] Targeting IBM Xforce
[*] IBM xForce Check: newstreamcapital.com
[-] IBM x-Force does not have entries for the domain!
[*] Targeting McAfee Trustedsource
[-] Getting anti-automation tokens
[*] Checking category for newstreamcapital.com
[!] Site categorized as:
[*] Targeting Websense
[-] Checking if you have any requests for the day.
[-] You have 2 requests left for the day.
[*] Checking category for newstreamcapital.com
[!] Site categorized as: Network Errors
[*] Targeting Cisco Talos
[*] Cisco Talos: newstreamcapital.com
[!] Uncategorized
```

<https://github.com/l0gan/domainCat>

```
root@plaintext:/opt/domainhunter# python3 domainhunter.py -s newstreamcapital.com
```



```
Expired Domains Reputation Checker
Authors: @joevest and @andrewchiles
```

```
DISCLAIMER: This is for educational purposes only!
It is designed to promote education and the improvement of computer/cyber security.
The authors or employers are not liable for any illegal act or misuse of this tool.
If you plan to use this content for illegal purpose, don't. Have a nice day!
```

```
[*] Downloading malware domain list from http://mirror1.malwaredomainlist.com/hosts.txt
[*] Fetching domain reputation for: newstreamcapital.com
[*] BlueCoat: newstreamcapital.com
[+] newstreamcapital.com: Finance
[*] IBM xForce: newstreamcapital.com
[+] newstreamcapital.com: Not found.
[*] Cisco Talos: newstreamcapital.com
[+] newstreamcapital.com: Uncategorized
[*] FortiGuard: newstreamcapital.com
[+] newstreamcapital.com: Finance and Banking
[*] Google SafeBrowsing and PhishTank: newstreamcapital.com
[+] newstreamcapital.com:
```

<https://github.com/threatexpress/domainhunter>

# Domain Category - Spear Phishing

```
$ python chameleon.py --proxy m --submit --domain foobar.com
```

[illegible]

```
[ -] Targeting McAfee Trustedsource
[ -] Getting anti-automation tokens
[ -] Checking category for foobar.com
[ -] Found category: - Personal Pages
[ -] Submitting URL for finance category
[ -] URL submitted, please wait up to 6 hours for categorisation
```

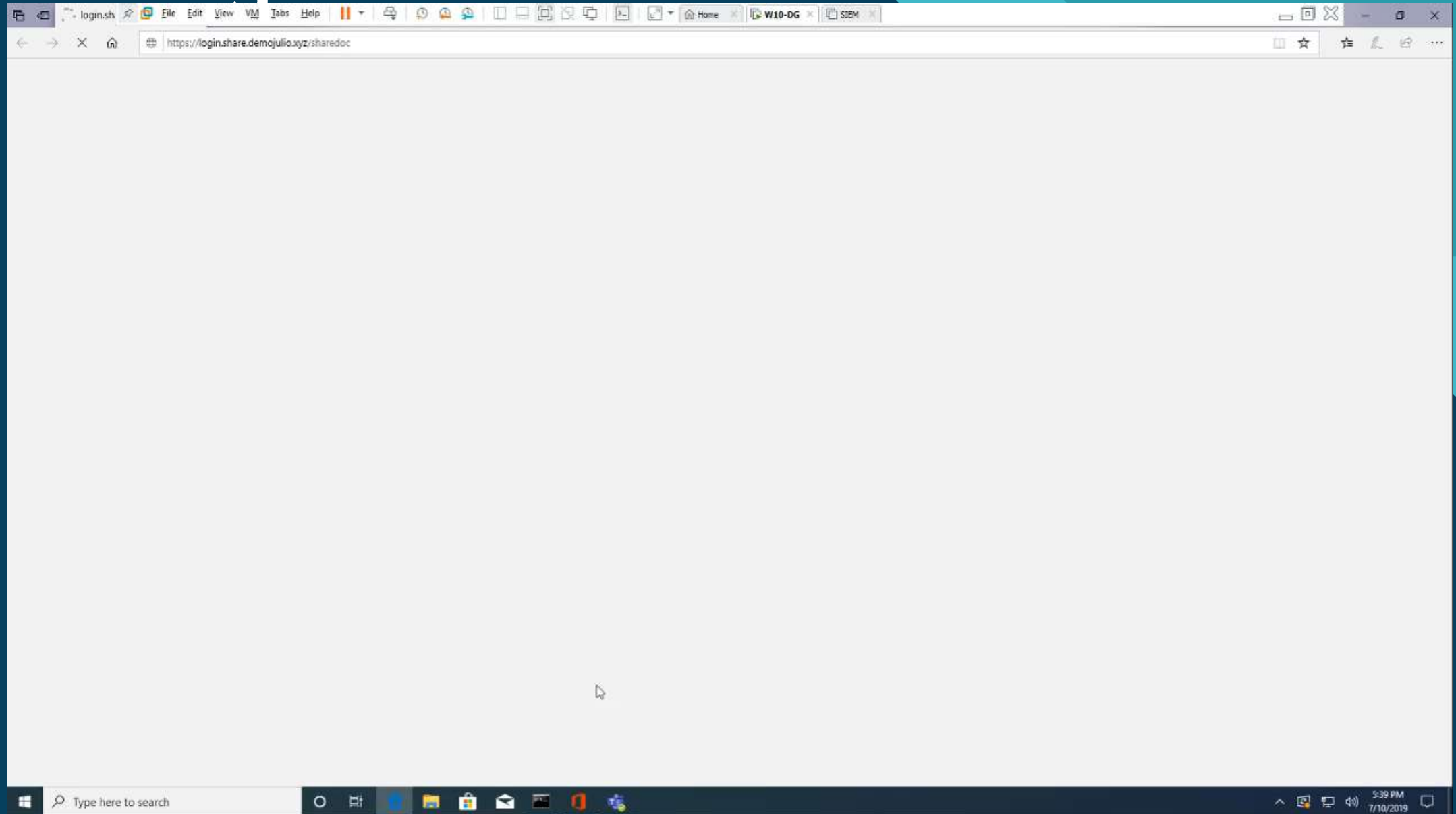
# Phishing 2FA



**evilginx2** is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

This tool is a successor to [Evilginx](#), released in 2017, which used a custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website. Present version is fully written in GO as a standalone application, which implements its own HTTP and DNS server, making it extremely easy to set up and use.

# Phishing 2FA



# Blue Team Tips



## Habilitar 2FA

Bueno contra:  
Password Spray  
Brute Force



## Definir Políticas de Passwords efectivas

“Cambiar las contraseñas regularmente no mejora la seguridad”



## Educación de sus usuarios

Bueno contra:  
Phishing  
Password Spray  
Brute Force



## Hunting

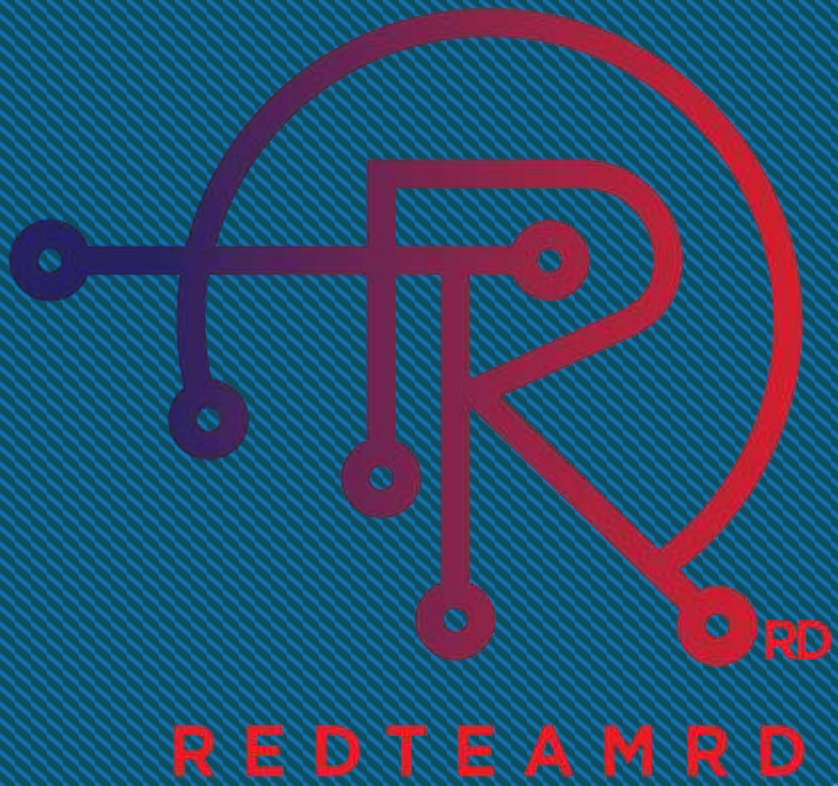
Creen habitos de buscar, investigar, revisen periodicamente los logs



## Conozcan su superficie de Ataque

Creen inventarios de los servicios disponibles que pueden ser usados para Password Spray, Phishing, Brute Force





¿Preguntas?

Gracias!!!