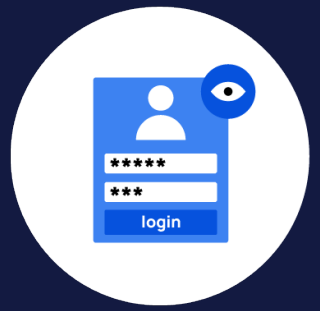
flare

The OpSec Hall of Shame

Little Meme Context

Quinn



4 cybercrime forums

10 suspicious/malware IPs

10 different stresser services

2 bruteforce txt

flare

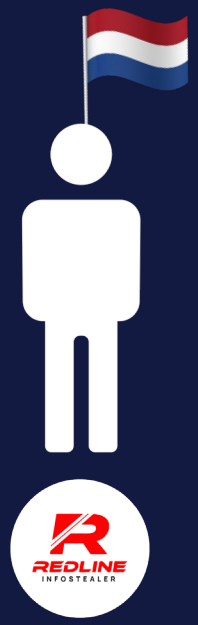
Quinn

https://www.nulled.to/topic/531764-fortnite-skin-checker-full-infos-tcm-fortnite-checker/page-1

```
Value: https://cracking.org/threads/fortnite-ass-fucker-a-fortnite-account-cracker-checker-cracked.254748/
==============
Name: search_term
Value: FORTNITE CHECKER
```

flare

Quinn



Address

Driving School

- Q***** V****** L******
- Date of Birth: 02/02/****

Favorite pornstar …

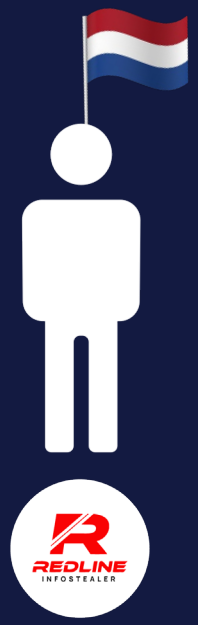
naughtyhotdaisy

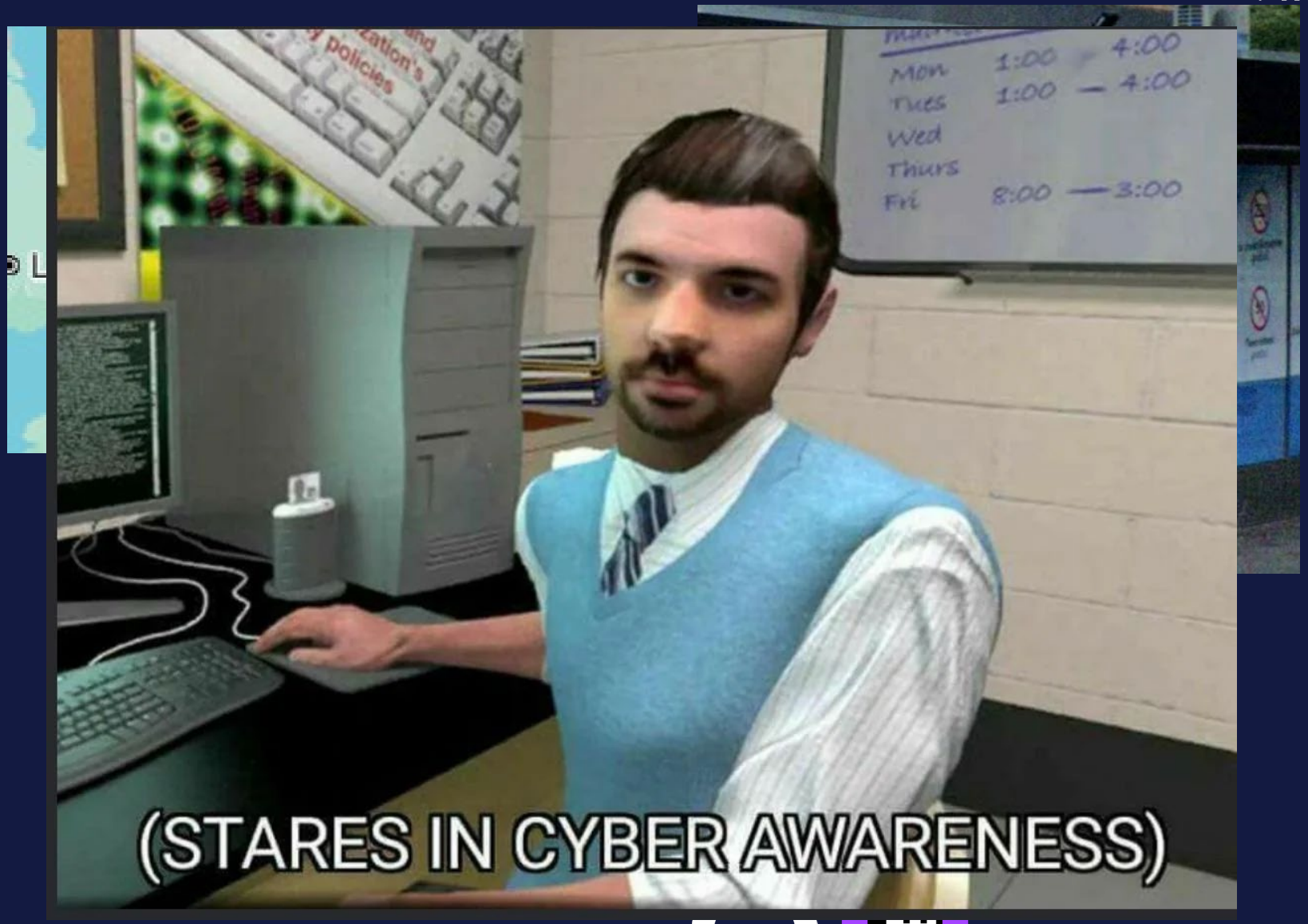
Social Media

Twitch and Github

flare

Quinn

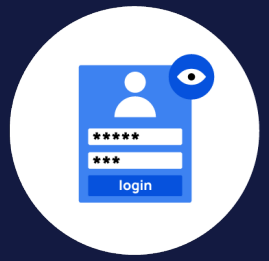

REDLINE
INFOSTEALER


Mon 1:00 — 4:00
Tues 1:00 — 4:00
Wed
Thurs
Fri 8:00 — 3:00
(STARES IN CYBER AWARENESS)

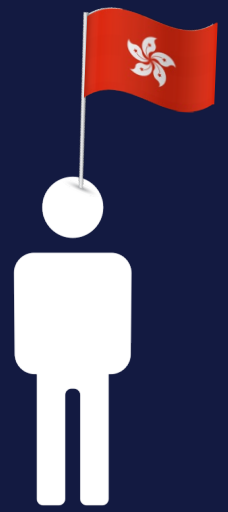
Lesson #2 :
OpSec Isn’t Included with the Malware Toolkit

flare

X. Yu

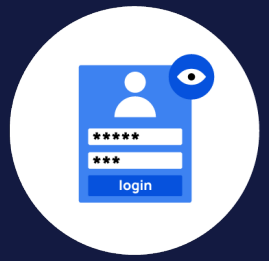


2 cybercrime forums

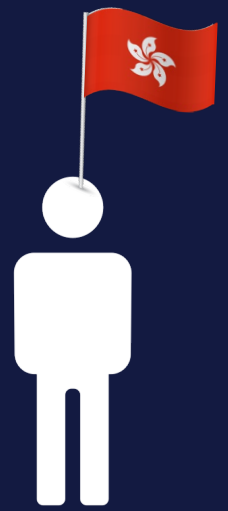


5 stresser services

X. Yu



2 cybercrime forums



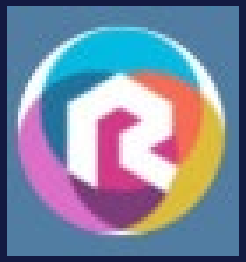
RisePro C2 IP

5 stresser services

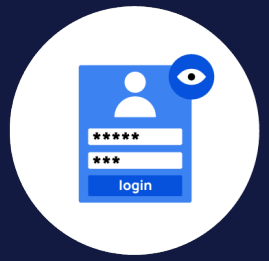
flare

X. Yu

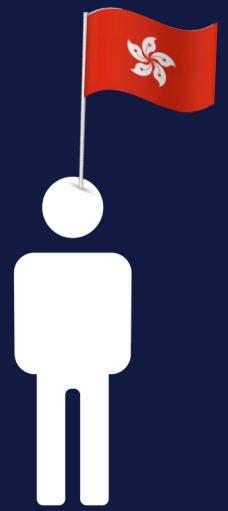
Stolen Accounts



RisePro C2 IP



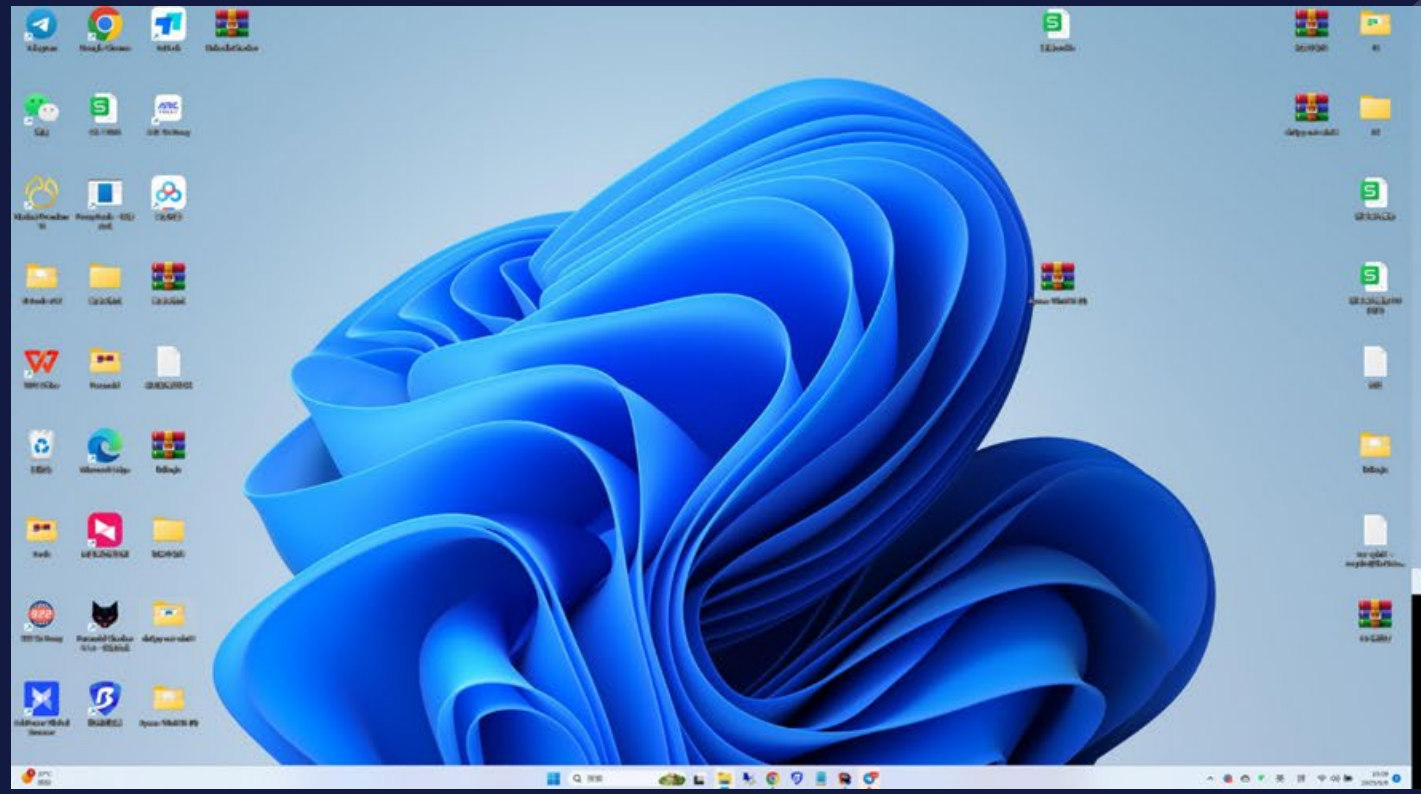
2 cybercrime forums

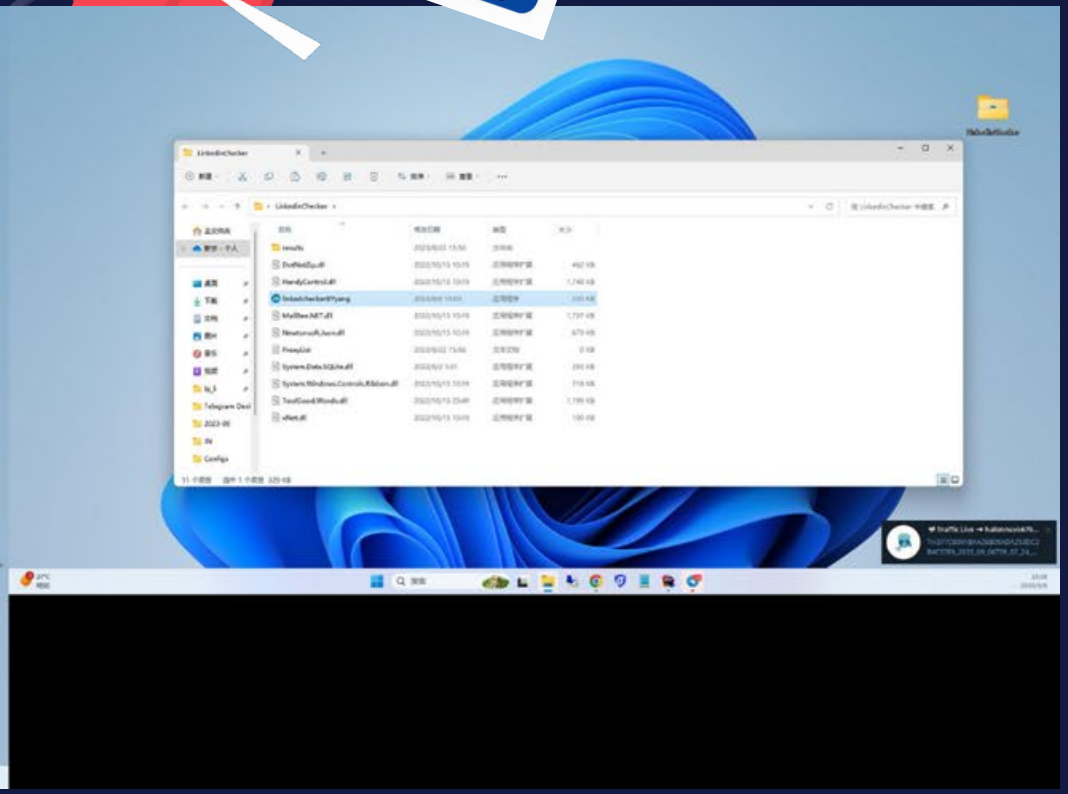


5 stresser services

Really Now…

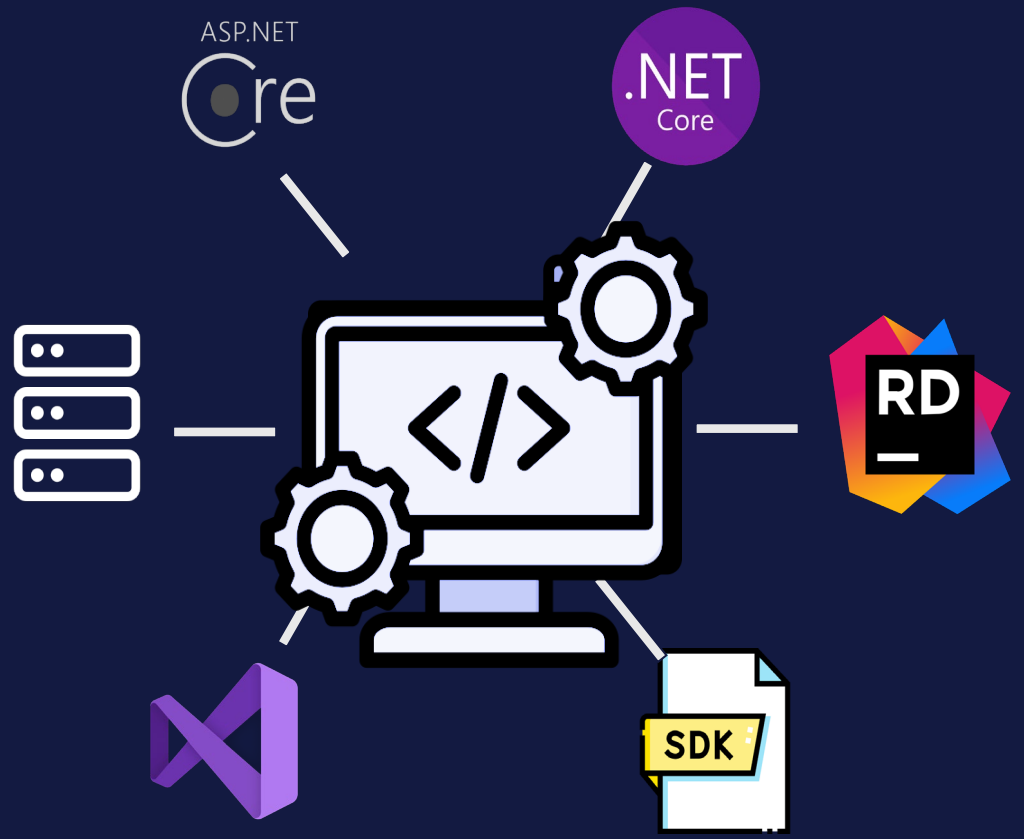
X. Yu





flare

X. Yu



) IntelliTraceProfilerProxy [15.0.21225.01]
) JetBrains Rider 2023.1 [231.8109.212]
) Microsoft .NET Framework 4.7.2 () [4.7.03062]
) Microsoft .NET Framework 4.7.2 Targeting Pack [4.7.03062]
) Microsoft .NET Framework 4.8 () [4.8.03761]
) Microsoft .NET Framework 4.8 SDK () [4.8.03761]
) Microsoft .NET Framework 4.8 SDK [4.8.03928]
) Microsoft .NET Framework 4.8 Targeting Pack [4.8.03761]
) Microsoft .NET Framework Cumulative Intellisense Pack for Vi
) Microsoft .NET Host - 7.0.10 (x86) [56.43.64668]
) Microsoft .NET Host FX Resolver - 7.0.10 (x86) [56.43.64668]
) Microsoft .NET Runtime - 6.0.14 (x64) [6.0.14.32123]
) Microsoft .NET Runtime - 6.0.21 (x86) [48.87.64667]
) Microsoft .NET Runtime - 7.0.10 (x86) [56.43.64668]
) Microsoft .NET Targeting Pack - 6.0.21 (x86) [48.87.64667]
) Microsoft .NET Targeting Pack - 7.0.10 (x86) [56.43.64668]
) Microsoft ASP.NET Core 6.0.21 - Shared Framework (x64) [6.0.
) Microsoft ASP.NET Core 6.0.21 Shared Framework (x86) [6.0.2
) Microsoft ASP.NET Core 6.0.21 Targeting Pack (x86) [6.0.21.23
) Microsoft ASP.NET Core 7.0.10 Shared Framework (x86) [7.0.10.
) Microsoft ASP.NET Core 7.0.10 Targeting Pack (x86) [7.0.10.233
) Microsoft ASP.NET Diagnostic Pack for Visual Studio [17.7.266.
) Microsoft ASP.NET Web Tools Packages 17.0 - CHS [17.0.30714
) Microsoft ASP.NET Web Tools Packages 17.0 - ENU [17.0.30714

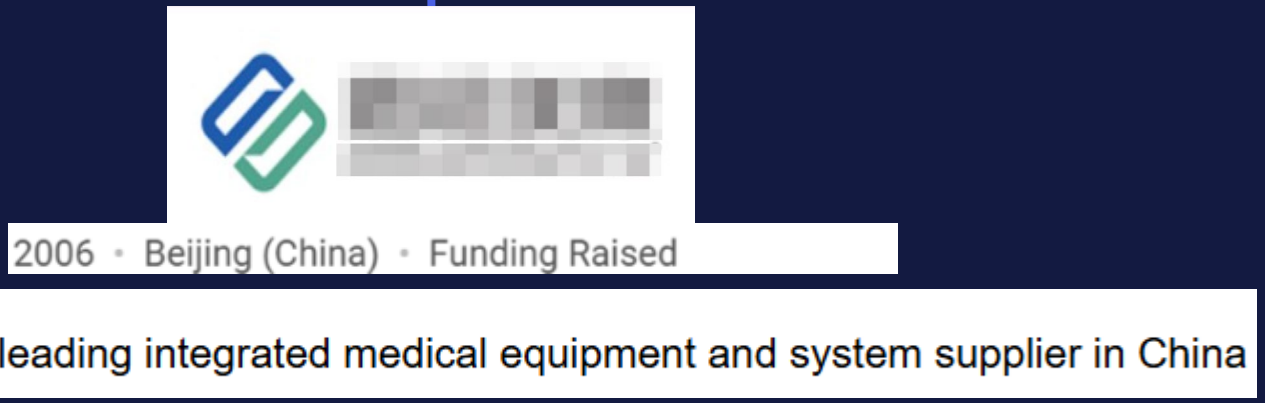
flare

X. Yu

Email: [*name*]@[*company name*].com

Username: [*company acronym*]_[*name*]

Access: mail/admin/oa.[company name].com



Email : marketing@company name.com
Website: www.company_name.com

flare

X. Yu

ccess

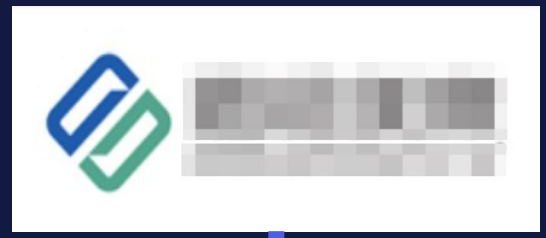
. x
. x
x

entials
tances

http://xy.skong.com:8080/gologin

flare

X. Yu



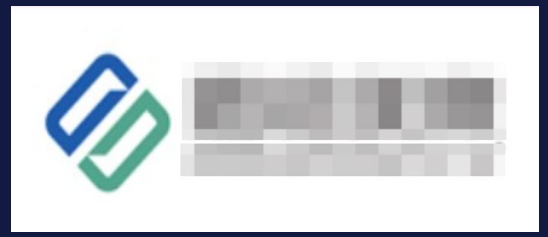
http://admin.skong.com/
http://admin.skong.com/gologin
http://alpha.skong.com:8080/gologin
http://alpha.skong.com:8081/gologin
http://devadmin.skong.com/gologin
http://devlogin.skong.com/login
http://docapi.skong.com/forwardlogin.htm
http://emtadmin.skong.com/gologin
http://gitlab.skong.com/users/sign_in
http://login.skong.com/login
http://proadmin.skong.com/gologin
http://prologin.skong.com/login
http://prowww.skong.com/search/gofindlist
http://proytadmin.skong.com/gologin
http://proytlogin.skong.com/login
http://sitadmin.skong.com/
http://sitadmin.skong.com/gologin
http://sitlogin.skong.com/login
http://sitshop.skong.com/
http://sitwww.skong.com/search/gofindlist
http://uatadmin.skong.com/
http://uatadmin.skong.com/gologin
http://uatlogin.skong
http://uatlogin.skong.com/login
http://uatwww.skong.com/search/gofindlist
http://webgladmin.skong.com/gologin
http://webgllogin.skong.com/login
http://xy.skong.com:8080/gologin

High Privilege Developper

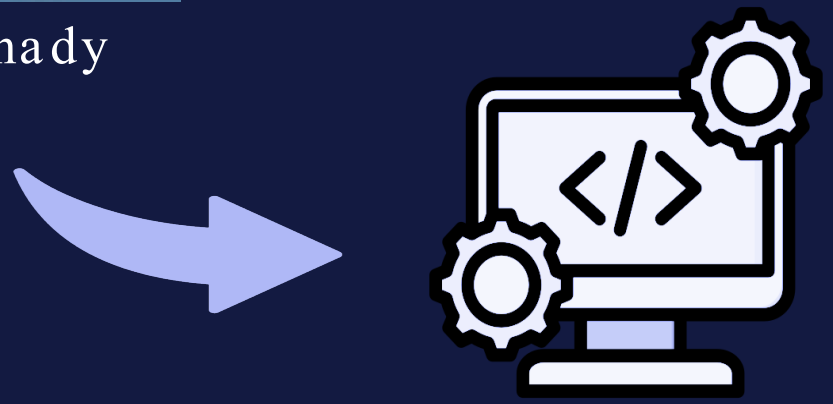
flare

X. Yu

Shady



Corporat
e



flare

X. Yu

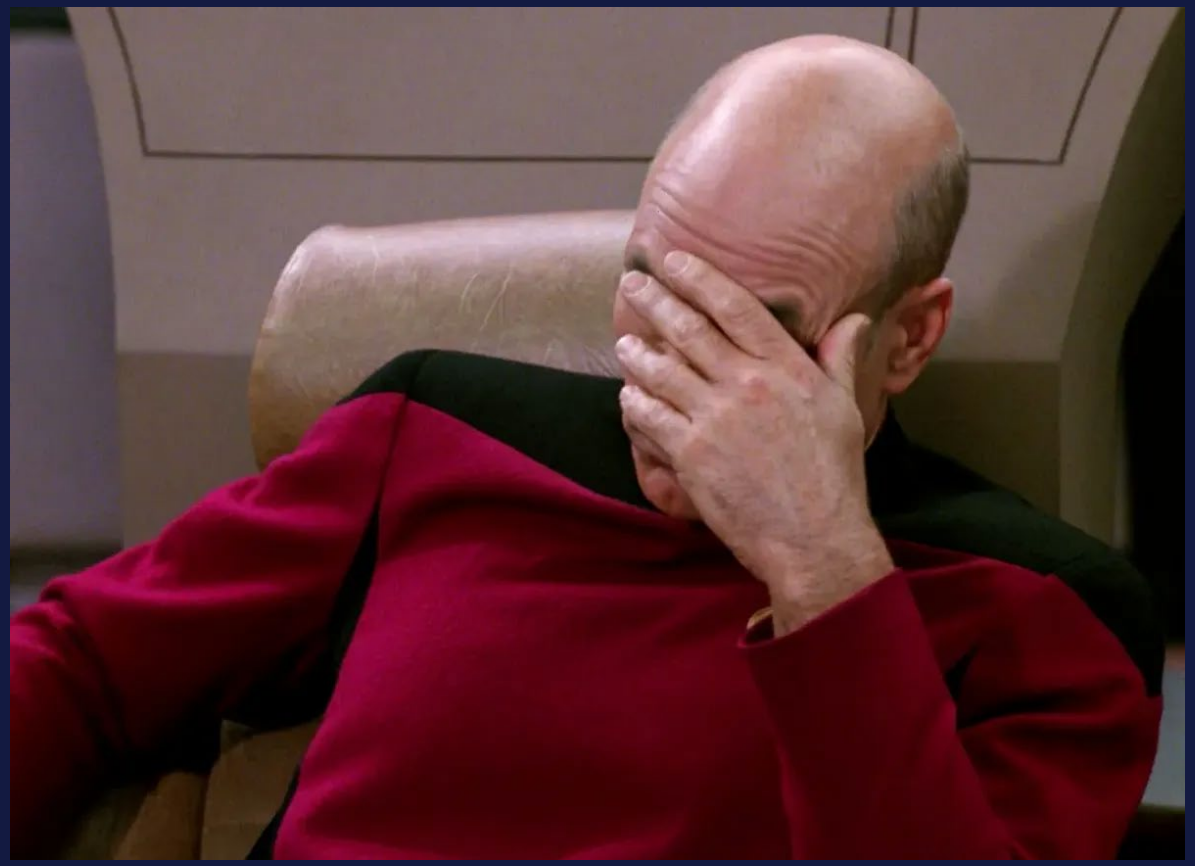
[redacted]

Legal

Do NOT use the same password for everything

7:01 PM
CST

Lesson #3:
Do NOT cross the streams - one device for business, another for your bad decisions



Estelle Ruellan
Cyber Threat Intelligence Researcher