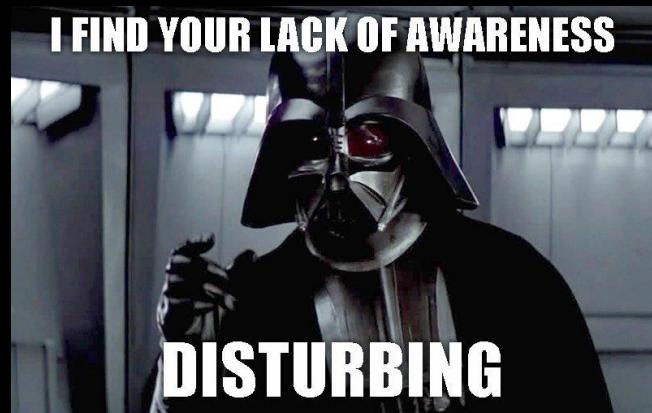


# The Silent Thief:

## Exploring the Dangers of Info Stealer Malware

Taylor Kaufman, Advanced Threat Hunter



# Disclaimer (CYB)



- This presentation is intended for educational purposes only and does not replace independent professional judgement.
- Statements of fact or opinions expressed are those of the presenter individually, and, unless expressly stated to the contrary, are not the opinions or positions of M&T Bank
- This presentation aims educate you on how to be aware of info stealer malware, the impacts of using MTB credentials outside of the bank, etc.
- The presenter cannot be held responsible if you decide, despite disclaimer, to embrace the dark side of the force, attempt to join a malware gang, and steal stuff on your own accord
- I do not own the rights to any Star Wars characters, memes, etc. as much as I would like to



# About Me

## Current Role

- Advanced Threat Hunter, M&T Bank
- CISSP, MS Azure Fundamentals, Network+, Security+ certified

## Previous roles

- 2.5 years - Risk process technical specialist III, M&T
- 2.5 years - Security Engineer, Seneca Gaming
- 1 year - IT support technician, Seneca Gaming

## Personal

- Graduated Buffalo State College class of 2015
  - B.S. Computer Information Systems
  - B.A. Television/Film arts
  - Minor, Philosophy
- InfraGard Buffalo and Technology advisory board member for the town of Grand Island
- Amateur boxer (and newly minted blackbelt kickboxer) out of Casal's boxing club
- Rucker (GRT & M&T VRG corporate liaison for the KIA memorial Roadmarch)



# What is InfoStealer Malware?

"Infostealer malware is a type of malware that is designed to steal sensitive information from a computer system. This information can include passwords, credit card numbers, bank account information, and other personal data."

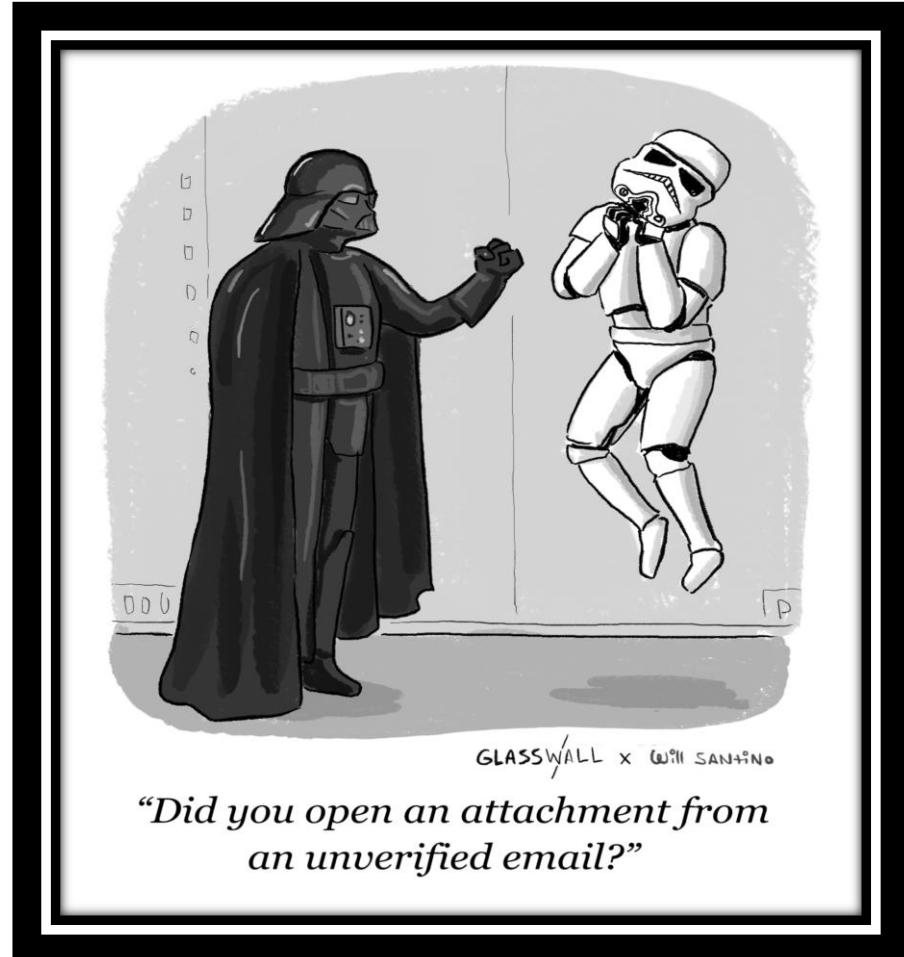
--Bard [experiment], AI, Google

"Infostealer malware is a type of malicious software that is designed to steal sensitive information from a victim's computer. This type of malware typically operates by covertly gathering and exfiltrating data from the infected system, which may include login credentials, financial information, personal identification details, or other sensitive data."

--ChatGPT, AI, OpenAI

"It is malware that steals information."

--Me, being lazy, M&T



*"Did you open an attachment from  
an unverified email?"*

# What is Stealer Malware After?

## Professional stealers

Stealers operated via Telegram in numbers

**34**

Number of Russian-speaking Telegram groups distributing info-stealing malware

**Redline, Racoon**

Stealers most frequently used by the members of the Telegram groups analyzed by Group-IB

**≈ \$ 5.8 mln**

Approximate value of stolen data in the cybercriminal underground

What stealers harvested in Jan-Jul 2022:

 Passwords  
**50,352,518** +80%\*

 Cookie files  
**2,117,626,523** +74%\*

 Crypto Wallets  
**113,204** +216%\*

 Payment cards  
**103,150** +81%\*



GROUP-IB, 2022

- Your OS information/version
- ISP information
- Active Cookies
- Your IP address
- FTP client information
- VPN credentials
- Browser cache
- Geolocation
- Browser fingerprints
- Cryptocurrency wallets
- Browser history
- Saved credit cards
- Telegram/Discord/etc.info

\*In comparison with Mar - Dec 2021



# Why is InfoStealer Malware after my stuff?

There is a price tag on everything! Most actors utilizing ISM are after a quick payday

- Steal money (crypto) directly
- Sell your credentials in bulk to the highest bidder (corporate creds = \$\$\$)
- Engage in fraudulent activities using your accounts
- Use your accounts to distribute more malware



# What do they do with your data once they have it?

- It depends!
- Mostly sell it. People who use InfoStealer as MaaS/SaaS (malware as a service/Stealer as a Service) are more interested in quick money. They'll sell stolen information in bulk or use a tiered subscription model.
  - Plenty of marketplaces to sell data (dark and clearnet sites)
  - Most people rent services or purchase data from others
- Highest price access \$\$\$: Corporation information
  - Threat actors sell and purchase data/fingerprints to gain access to corporate resources.
- Pivot with your credentials to other websites and services (why password reuse is terrible) to steal more data or distribute other malware services, including, but not limited to ransomware



Admin Access to the main server of a medical clinique from US  
RDP Access  
PosSystems + DataBase \* over 600GB \* of data  
Over 30 computers in the network  
1000\$  
Blitz : 900\$  
Escrow Accepted

Admin access to : WebServer +  
Start : 5000\$  
Step :

# How does InfoStealer malware work?

The malware is delivered via phishing, drive by downloads, you downloading it, exploiting open vulnerabilities, etc.

Info stealers may use many methods of data acquisition such as:

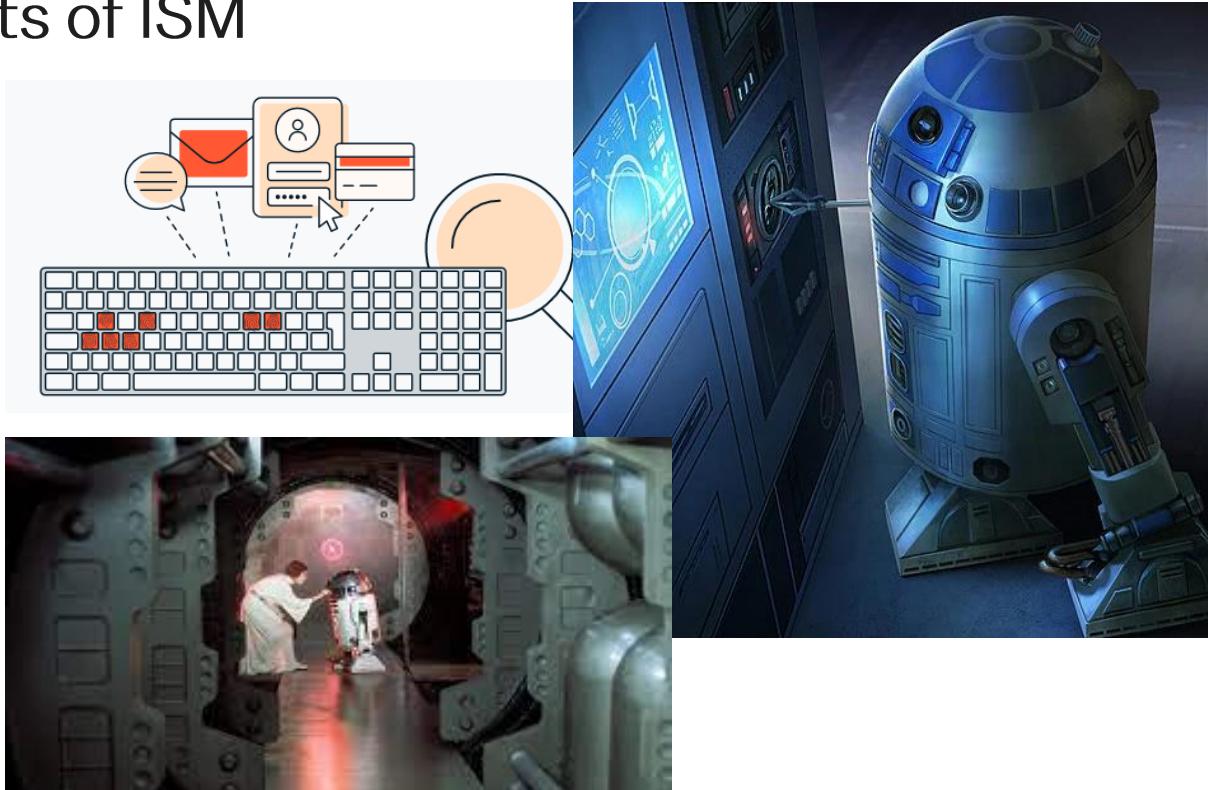
- Hooking browsers (and sometimes other applications) and stealing credentials that are typed by the user
- Using web injection scripts that are adding extra fields to web forms and submitting information from them to a server owned by the attacker
- Form grabbing (finding specific opened windows and stealing their content)
- Keylogging
- Stealing passwords saved in the system and cookies



# What constitutes the ISM makeup?

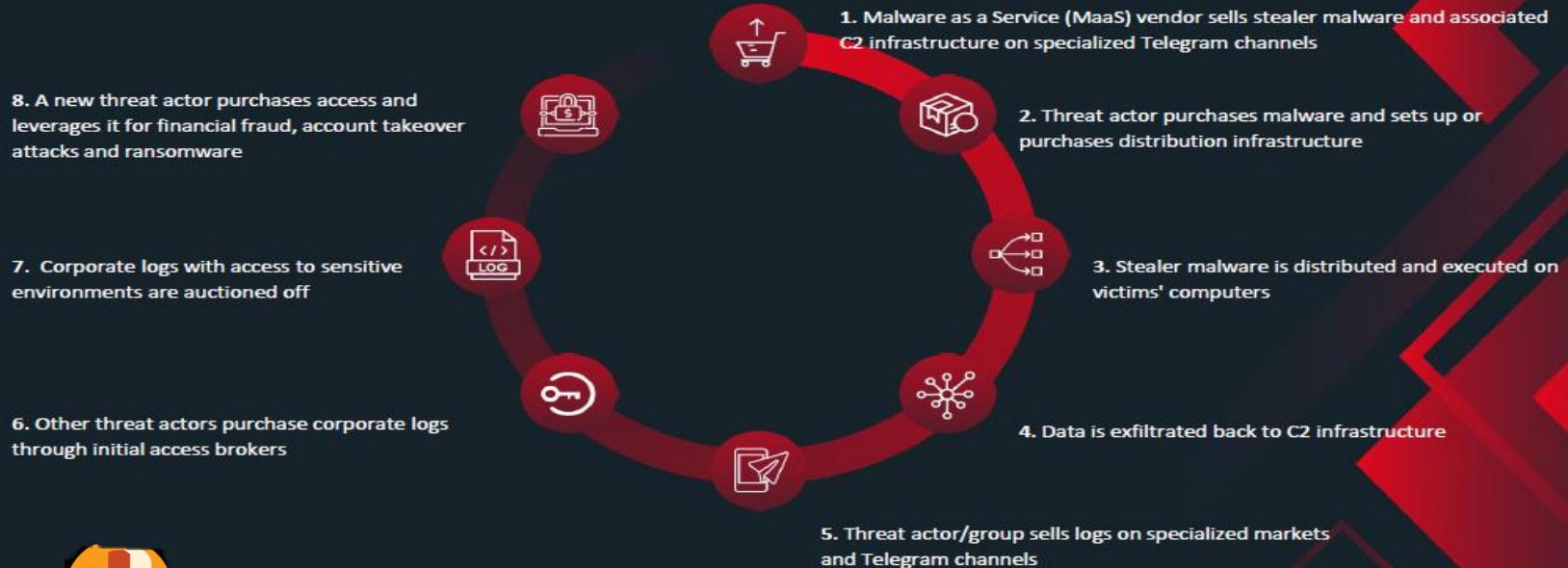
## Different components of ISM

- Keylogger
- Credential Stealer
- Clipboard Stealer
- Form Grabber
- Screen Scraper
- Webinjects
- Skimmers
- C2
- Secondary payloads



# Lifecycle

## Lifecycle of a Stealer Malware Attack



# Execution

1. Stealer malware is downloaded or installed through illicit ads, freeware, or phishing emails
2. Typically a .exe is downloaded with a powershell script, which is used to obfuscate the malicious code
3. Persistence mechanisms are added such as creating registry keys and adding itself to startup
4. Junk files are created to make detection & analysis more difficult

5. Malware begins attempting to establish live communication with C2 Infrastructure
6. Additional modules are remotely downloaded from C2 infrastructure
7. Host information, screen capture, and initial logs are sent back to C2 infrastructure
8. Continuous data exfiltration from the infected machine begins

# Redline Stealer in action





SEVEN  
ONE TECH

Recycle Bin NWZAP... NEBFQQY... ZQJXMQ...

Acrobat Reader DC PWCCAW... NEBFQQY... ZQJXMQ...

Excel 2016 Word 2016

Microsoft Edge QCFWYSK PIVPAGEAA...

Google Chrome ZQJXMQ PWCCAW...

redLine.exe DUUDTUB... QNCYCDFI...

EIVQSAOTAQ EFOYFBOL... QNCYCDFI...

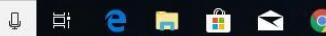
GRXZDKK GAOBCVIQ... QNCYCDFI...

IPKGELNTQY IPKGELNTQ... SQSJKEBW...

KLIZUSIQEN LSBIHQFDV... SOSJKEBW...

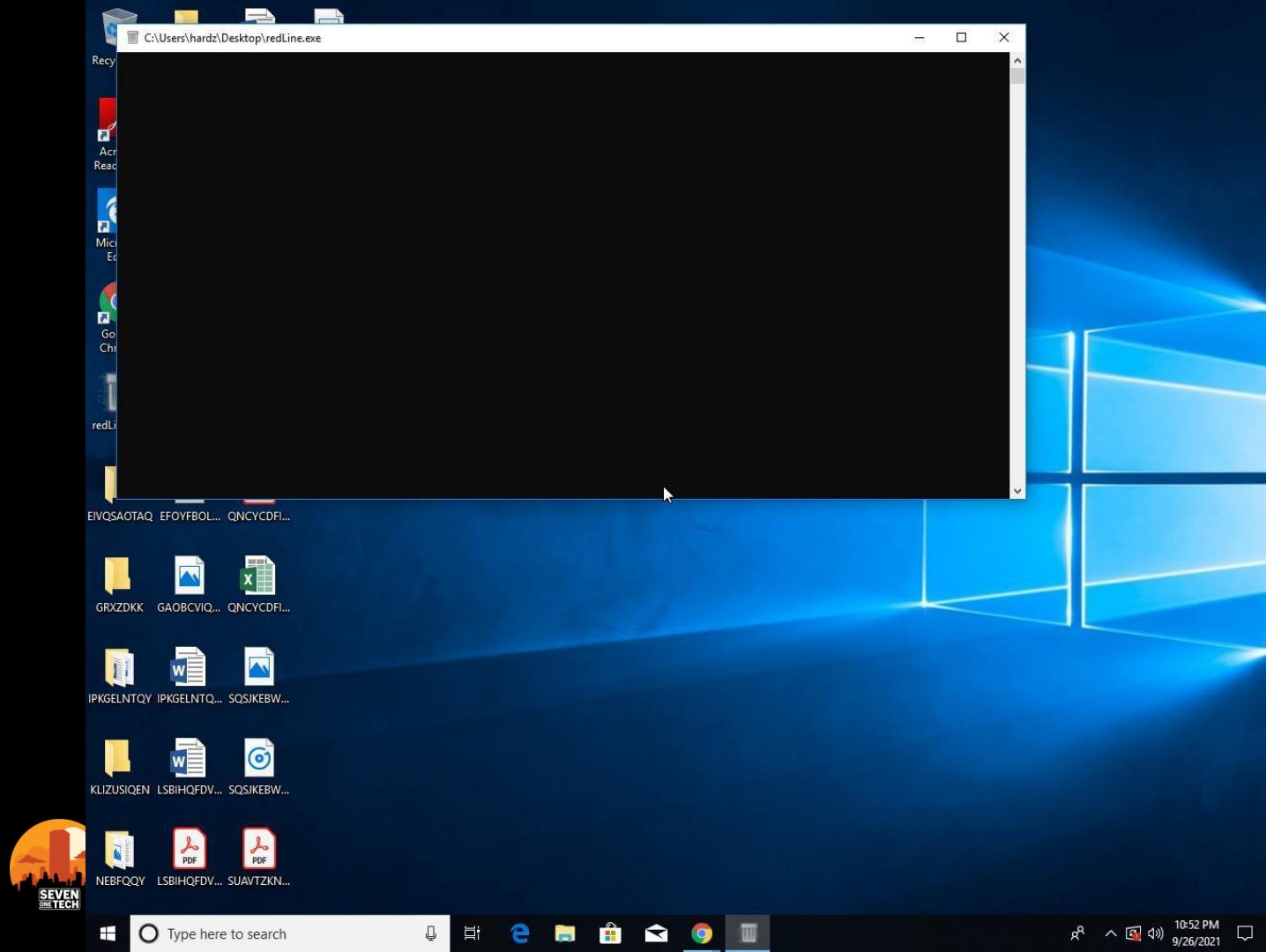
NEBFQQY LSBIHQFDV... SUAVTZN...

Type here to search



10:54 PM  
9/26/2021

M&T Tech



M&T Tech



SEVEN  
ONE TECH

Recycle Bin NWZAP... NEBFQQY... ZQJXMQ...

Acrobat Reader DC PWCCAW... NEBFQQY... ZQJXMQ...

Excel 2016 Word 2016

Microsoft Edge QCFWYSK PIVFAGEAA...

Google Chrome ZQJXMQ PWCCAW...

redLine.exe DUUDTUB... QNCYCDFI...

EIVQSAOTAQ EFOYFBOL... QNCYCDFI...

GRXZDKK GAOBCVIQ... QNCYCDFI...

IPKGELNTQY IPKGELNTQ... SQSJKEBW...

KLIZUSIQEN LSBIHQFDV... SOSJKEBW...

NEBFQQY LSBIHQFDV... SUAVTZN...

Type here to search



10:54 PM  
9/26/2021

M&T Tech

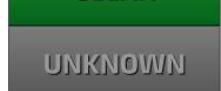
## General Information

Sample Name:	redLine.exe
Analysis ID:	490972
MD5:	3b3b09c0f40c3c2b1...
SHA1:	34751fcfd32458507...
SHA256:	2519257a94977d7b...
Tags:	exe redline RedLineStealer
Infos:	

Most interesting Screenshot:



## Detection

 <b>MALICIOUS</b>	
 <b>SUSPICIOUS</b>	
 <b>CLEAN</b>	
 <b>UNKNOWN</b>	
 <b>RedLine</b>	
Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

## Signatures

- Yara detected RedLine Stealer**
- Found malware configuration
- Multi AV Scanner detection for submitted...
- Detected unpacking (overwrites its own ...)
- Tries to steal Crypto Currency Wallets
- Queries sensitive video device informatio...
- Queries sensitive disk information (via W...
- Tries to harvest and steal browser inform...
- Uses 32bit PE files
- Queries the volume information (name, s...
- Contains functionality to check if a debug...
- Contains functionality to query locales inf...
- May sleep (evasive loops) to hinder dyna...
- Checks if Antivirus/Antispyware/Firewall ...
- Uses code obfuscation techniques (call, ...
- Internet Provider seen in connection with...

## Classification





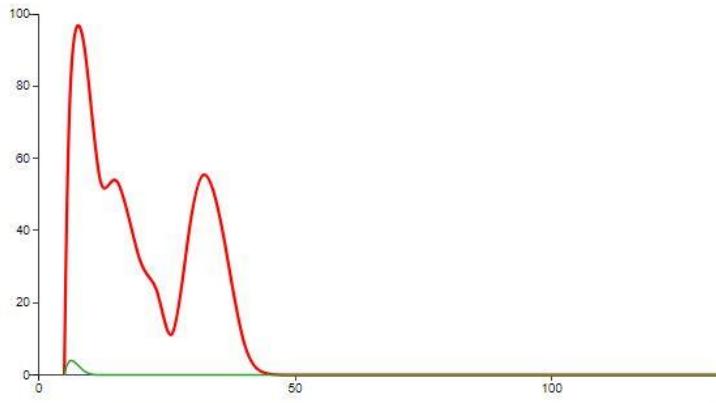
## IPs



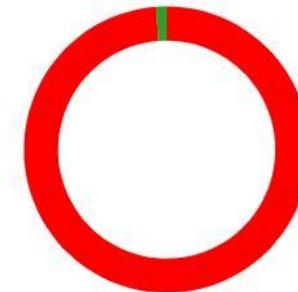
Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.9.20.20	iT1f2b2uQG.exe	Get hash	malicious	<a href="#">Browse</a>	
	4by0l2GYt1.exe	Get hash	malicious	<a href="#">Browse</a>	
	xCwGNck6H.exe	Get hash	malicious	<a href="#">Browse</a>	
	ec0d0t6b46.exe	Get hash	malicious	<a href="#">Browse</a>	
	aG1d7FdZey.exe	Get hash	malicious	<a href="#">Browse</a>	
	VnKKRx4E3c.exe	Get hash	malicious	<a href="#">Browse</a>	
	MAauX39db3.exe	Get hash	malicious	<a href="#">Browse</a>	
	p2r5ojd3Ec.exe	Get hash	malicious	<a href="#">Browse</a>	
	OmlEwqzYLr.exe	Get hash	malicious	<a href="#">Browse</a>	
	ae48GWjkLE.exe	Get hash	malicious	<a href="#">Browse</a>	
	VhikmSr52Q.exe	Get hash	malicious	<a href="#">Browse</a>	
	SLISRI5MIB.exe	Get hash	malicious	<a href="#">Browse</a>	
	vc9TwhTemB.exe	Get hash	malicious	<a href="#">Browse</a>	
	h28sBGvX8o.exe	Get hash	malicious	<a href="#">Browse</a>	
	8XoievJlmd.exe	Get hash	malicious	<a href="#">Browse</a>	
	D7fedJj8na.exe	Get hash	malicious	<a href="#">Browse</a>	
	IT0uVNcO30.exe	Get hash	malicious	<a href="#">Browse</a>	
	CHMr3BVD15.exe	Get hash	malicious	<a href="#">Browse</a>	
	2N7AR7LtmЬ.exe	Get hash	malicious	<a href="#">Browse</a>	
	hXyGaeSOy7.exe	Get hash	malicious	<a href="#">Browse</a>	



### CPU Usage

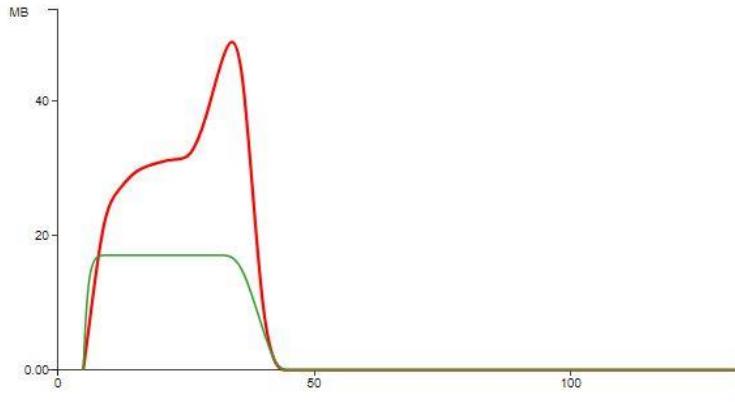


● redLine.exe  
● conhost.exe

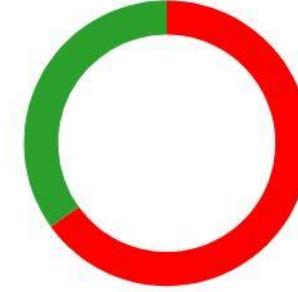


💡 Click to jump to process

### Memory Usage

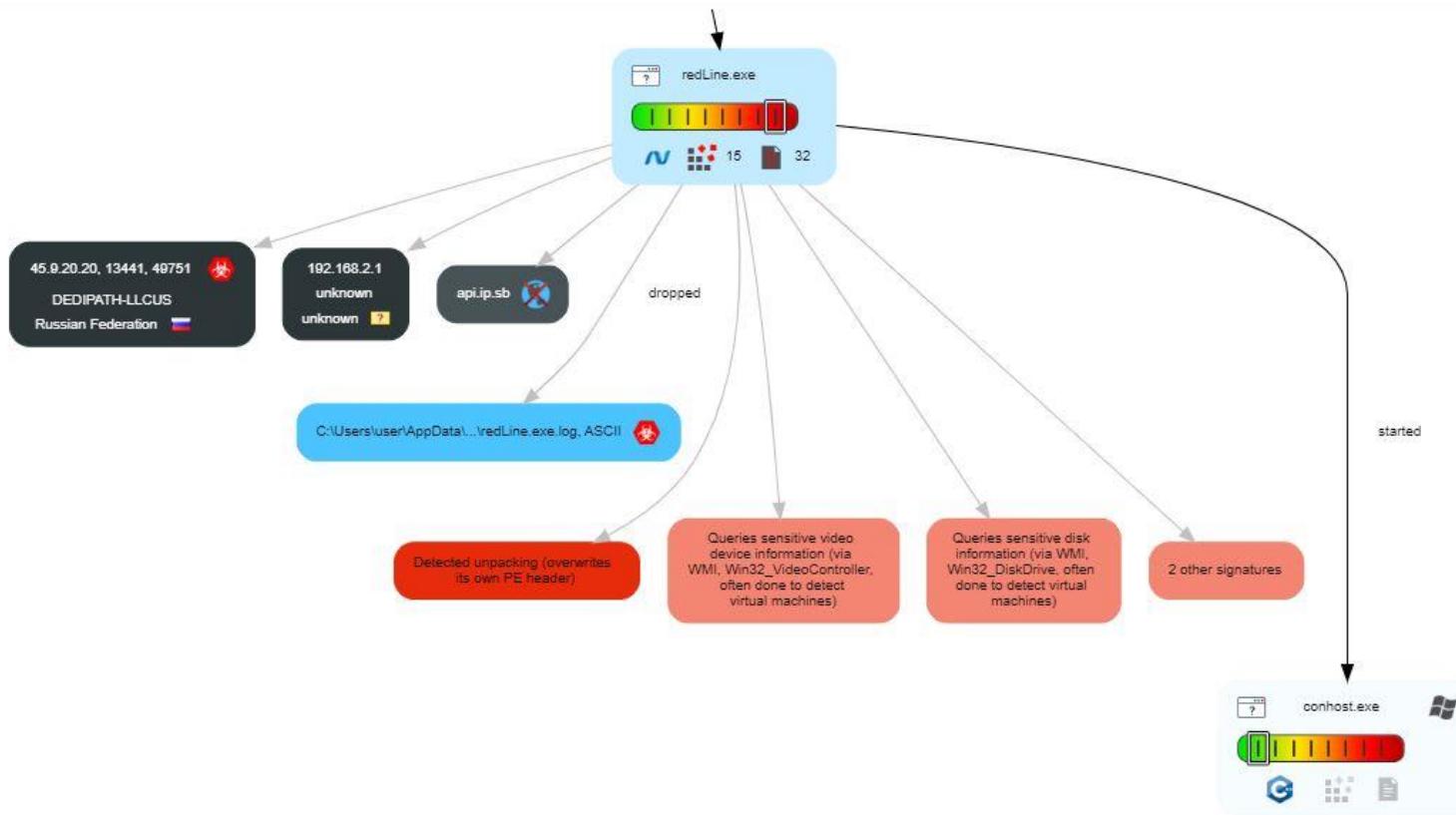


● redLine.exe  
● conhost.exe

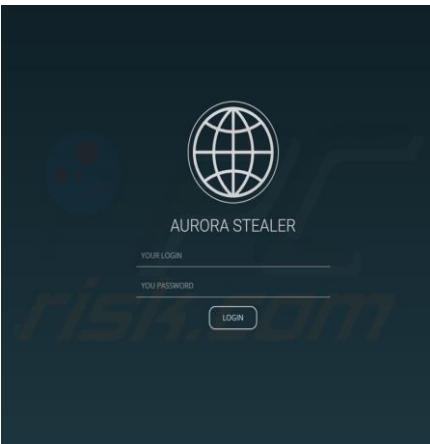


[Hide Legend](#)

- Legend:
- Process
  - Signature
  - Created File
  - DNS/IP Info
  - Is Dropped
  - Is Windows Process
  - Number of created Registry Values
  - Number of created Files
  - Visual Basic
  - Delphi
  - Java
  - .Net C# or VB.NET
  - C, C++ or other language
  - Is malicious
  - Internet



# The Main Families\*



Feb 19, 2020

REDGlade Local

Joined: Feb 13, 2020

Messages: 102

Reaction score: 28

Points: 372

WHEN PURCHASING THROUGH THE PM OF THE FORUM OR THE GUARANTOR OF THE FORUM 20% DISCOUNT FOR ALL TYPES OF SERVICES

Write only and only here <https://t.me/NEWREDLINE> and require confirmation through the PM of the forum

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

Build features:

- 1) Collects from browsers:
  - a) Login and passwords
  - b) Cookies
  - c) Autofill fields
  - d) Credit cards
- 2) Supported browsers:
  - a) All browsers based on Chromium ( Even the latest Chrome version )
  - b) All browsers based on Gecko ( Mozilla, etc.)
- 3) Collecting data from FTP clients, IM clients
- 4) Customizable grabber file according to the criteria Path, Extension, Search in subfolders (can be configured for the desired cold wallets, steam, etc.)
- 5) Sample by country. Configuring a black list of countries where the build will not work
- 6) Configuring anti-duplicate logs in the panel
- 7) Collects information about the victim's system:  
IP



\*Not an all-encompassing list

M&T Tech

# The Trader Outposts of Stolen Information

This screenshot shows the Genesis platform's interface. On the left, a sidebar lists various sections like Dashboard, Genesis Wiki, News, Bots, Generate FP, Orders, Purchases, Payments, Tickets, Software, Profile, Invites, and Logout. The main area displays a list of seized bots. One bot, labeled 'F5C20E55' with a red 'new' badge, has a large watermark across its interface reading 'THIS WEBSITE HAS BEEN SEIZED'. Below this, the bot's details are shown: 'BOT NAME: /api/20.leya.com' with a 'CC' badge, 'Filter bot name', and a timestamp '2021-08-20 12:20:21'. Another bot, 'D1854F88E5', has a timestamp '2020-08-21 02:20:21' and '2x'. A third bot, '3796BE0F66FD2C4D66', has a timestamp '2020-10-31 23:38:34' and '2x'. The interface also includes sections for Steam, Instagram, and various logos.

This screenshot shows a dark-themed dashboard. At the top, it says 'Type: Topic | 12/19/2021, 12:01:12 AM | Mentions: 96/222' and 'Phishing (589)'. Below this, a message reads '162 [REDACTED] | 12/19/2021, 5:35:33 AM CITI BANK LOG + Credit Card!'. The main content area displays a seized log entry: 'Log + full name + Access + Phone + Adress + Ip + DOB + MMN + SSN + ATM-PIN + Carrier-pin Credit Card (542418)'. Below this, a 'BIN : 542418' section is shown with details: 'Carrier pin : Yes (unverified)', 'Atm pin : Yes (verified)', 'CVV&exp : Yes', 'Name : Andre', 'Gender : Male', 'Carrier : Cing', and 'state : NY'.

This screenshot shows a dark-themed marketplace interface. At the top, it says 'RUSSIAN MARKET'. Below this, there are sections for 'Stalker', 'System', and 'Country'. The 'Stalker' section lists various users with their names and country codes. The 'System' section shows a list of items for sale, such as 'PSD INDUSTRIAL PASS', 'PSD PROFESSIONAL PASS', 'PSD CALIFORNIA PASS', 'PSD China Passport 2013+', 'PSD Belize DX +D+PASS', 'PSD Canada DX +PASS', 'PSD Mexico DX +PASS', 'PSD Wisconsin Driver License', 'Alabama NEW PSD', 'DL Texas PSD new', 'BRANICE EU (EU) KYC', 'Business Full+Sticker+IC', 'Business Full+Sticker+IC', 'Business PRO', 'Business PROS', and 'Residential OpenVPN'. Each item has a price and a 'Contact seller' button. A central banner says 'ACCEPT SCAM' and 'KRAKEN EXCHANGE' with a Russian message 'Нужно отмечать для запуска CC/Cash!'.

# The Customer Service of Initial Access Brokers

Initial Access Brokers (IABs) are the white glove service for cybercriminals.

They take stealer logs a step further by:

- Validating access
- Potentially move laterally through networks and services
- Enriching data for further context (with third-party enrichments solutions often used by corporate sales teams)

A screenshot of a forum post from a user named 'plymouth'. The post was made on Jan 16, 2023. The user's profile picture is a logo for 'plymouth CD-диск'. Below the profile picture, the user is identified as 'Пользователь' (User). The user joined on Jul 30, 2022, has 12 messages, a reaction score of 4, one escrow deal, and a deposit of 0.02 B. The post content reads: "We're giving away free weekly tests! Contact us!" At the bottom right of the post, there are options to 'Like', 'Quote', and 'Reply'.

A screenshot of a forum post from a user named 'inthematrix1'. The post was made on November 6. The user's profile picture is a portrait of a person with a mask. Below the profile picture, the user is identified as 'byte'. The user has a paid registration of 15, 16 posts, and joined on 06/25/20 (ID: 105713). The user's activity is listed as 'кардинг / carding'. The user's deposit is 0.002488 B. The post content includes user details: Revenue : 50kk, Country : Chile, Industry : Insurance and leasing, Local Administrator rights, AV : Sophos. It also lists transaction details: Start : 1000\$, Step : 200\$, Blitz : 2000\$. The post concludes with a note: "Dealing only with people with reputation from the forum or users that have deposits , new users i ignore Escrow accepted PPS : 4h".

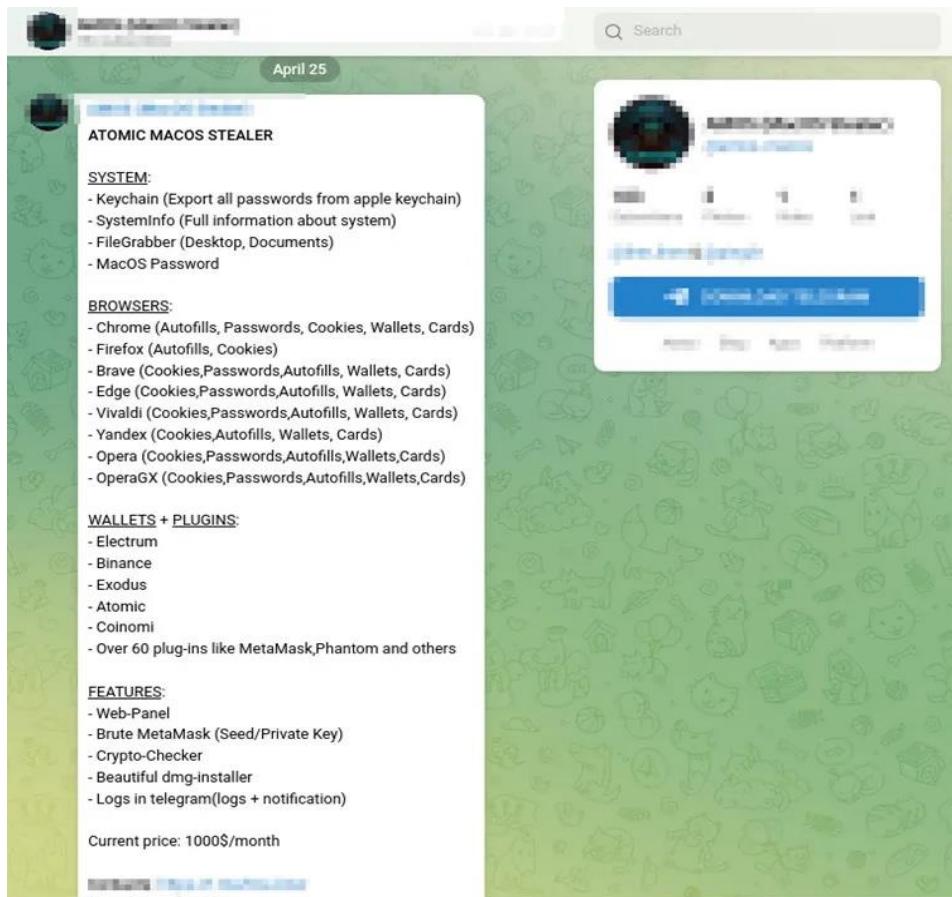


# “I use a Mac. I am safe. . .”



# Mac InfoStealer

- New (April '23) Atomic macOS Stealer (AMOS) malware as it was advertised for sale on Telegram.
- The threat actor marketing it is regularly updating the malware and is charging \$1,000/month for it.
- AMOS can compromise a long list of items including iCloud Keychain passwords; the macOS system password; cookies, passwords, and credit card details from Chrome, Firefox, Brave, Edge, Opera, and more.
- The malicious party selling the malware as a service also includes a web panel, Brute MetaMask tool, logs in Telegram with notifications, and more to buyers.



# Why is this such a profitable industry?

And why hasn't anyone stopped this yet??



| Log ID : [REDACTED]  
| Site : BOA  
| Account Balance : 1400 \$  
| Login : Login Info ✓ Can Login ✓  
| Mailaccess : netzero.com - Can Login ✓  
| Billing : Cheboygan County, MI, 49799  
| Card : x Credit - 440066 - LIVE CARD ✓  
| Carrier :  
| Zelle : Unknown 8  
| Wire : Unknown 8  
| IDentity : Driver's license  
| Proof :  
| Additional Info : [ Email Access - Email Access - Email Access - Pin-  
ATM - DOB : 1953 - MMN - Phone - SSN - ]  
| Info By seller : FRESH LOG CREDIT CARD ! CEK Private Information  
For Buyer  
| Price 110 \$  
> Buy it from [REDACTED]

- New markets consistently spring up when old ones are taken down.
- Markets or channels are hosted in countries not receptive to take down/prevent the crimes
- Monitoring listings manually is almost impossible
- The price is good—bulk logs can be sold for as little as \$10. Some sell subscriptions to channels/platforms and allow access to a minimum of new logs per day
- IABs can resell infected devices for thousands
- Crypto difficult to track



# How do I keep myself safe?

## Personal Devices/Accounts

- Don't click or download anything suspicious
- Use a unique/different password for all your accounts
- Regularly check to see if your account or password 'has been pwned'  
<https://haveibeenpwned.com/>
- Sign up for identity protection services
- Keep your systems patched/up to date (including browsers, applications, etc.)
- Turn on MFA/OTP/secondary auth protections

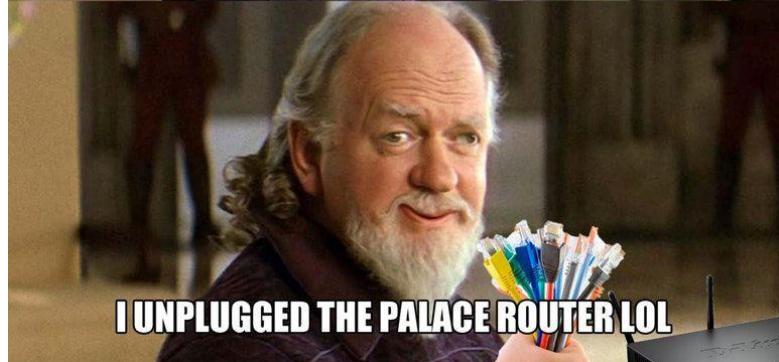
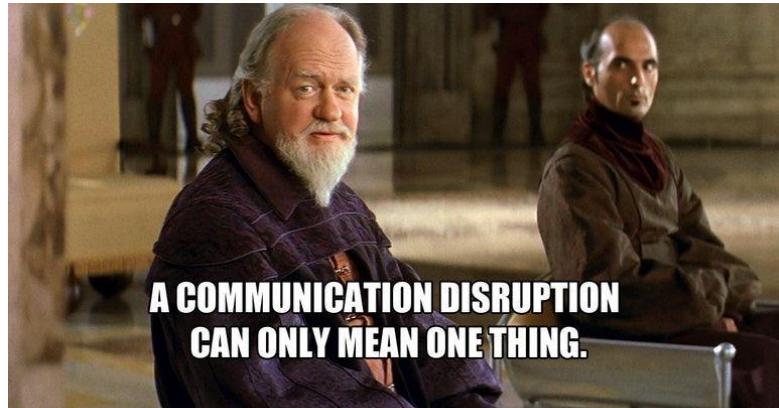


## Work/M&T Bank accounts

- Do not use your M&T account/email to sign up for anything sketchy
- Do not use the same password across corporate and personal devices
- Alert Cybersecurity ([CSOC@mtb.com](mailto:CSOC@mtb.com)) immediately if you suspect a compromise
- Do not click any malicious links or download any unapproved applications to your work machine.
- If you see something, say something
- Don't get mad at the awesome tech folks who force reboot your machine after patching it

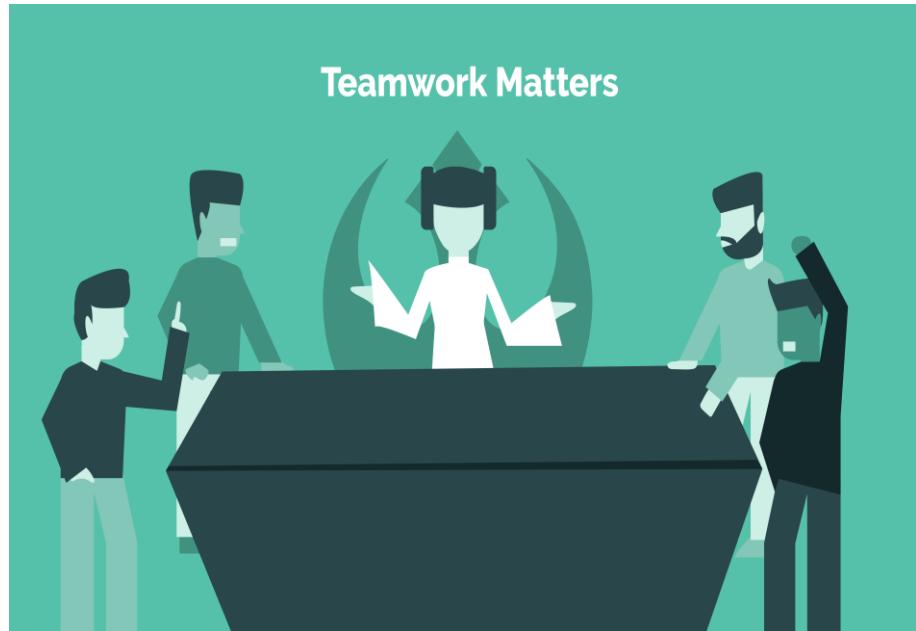
# How the cyber industry disrupts ISM

- Disrupt the supply chain
- Monitor infected device markets and set up automated processes to detect newly staged attack infrastructure; conduct take downs with LEO
- Utilize web & email filtering to screen malicious sites and emails
- Layer technical and governance controls

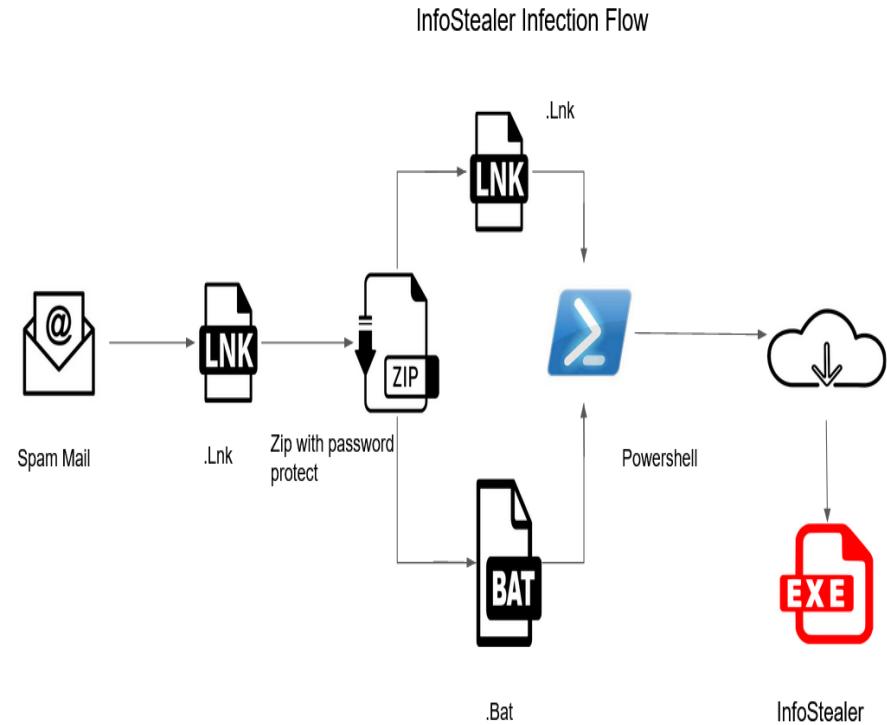
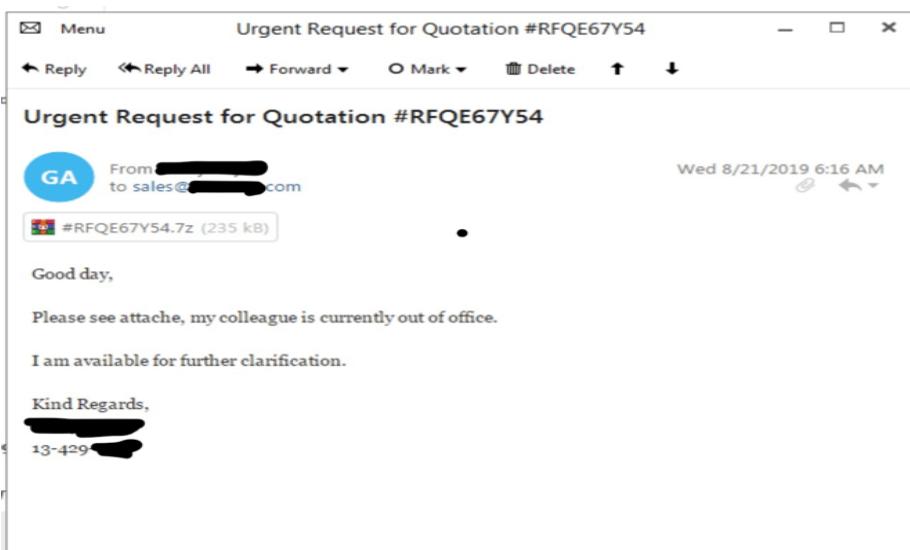
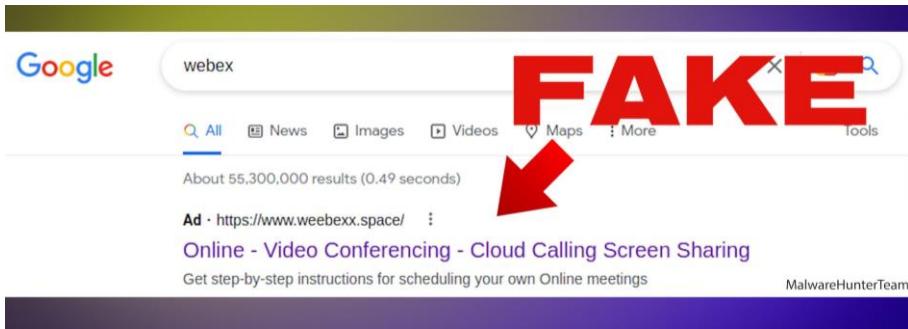


# What is M&T doing to prevent InfoStealer infections?

- Threat Intel monitoring for stolen credentials (both customers and employees)
- CSOC alert monitoring for unusual logins and malicious downloads
- Phishing email monitoring and protections (both report mailbox and vendor provided intel/response)
- Threat Hunting on new techniques and campaigns
- Vulnerability risk management and regular patching cadences
- Proxy blocks and prevention of downloads from malicious sites
- Annual employee training and phishing tests



# How to recognize InfoStealer



# Case Study: Linux Tech Tips YT hack

March '23: Linus Tech Tips (LTT) channel was hacked and terminated for showing crypto-scam videos. With over 15.8 million subscribers, the channel was among the largest technology-focused channels on the platform.



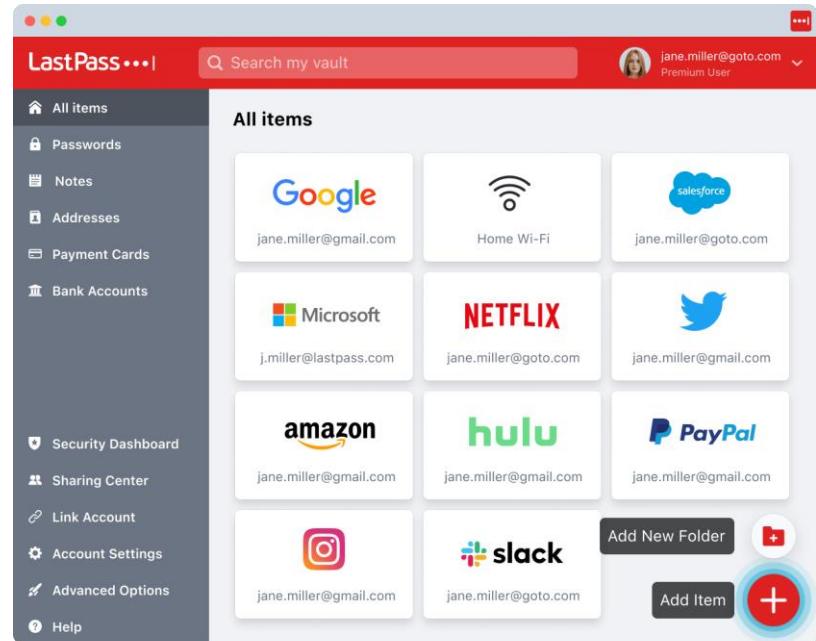
“Someone on the Linus Media Group’s team downloaded “what appeared to be a sponsorship offer from a potential partner” and launched the included PDF with the terms of that offer. This offer actually contained malware that accessed “all user data from both their installed browsers” — including session tokens — which effectively gave the bad actor “an exact copy” of the browsers that they could export and use to wreak havoc without needing to enter security credentials.”

# Case Study: LastPass Hack

March '23: The massive breach at LastPass was the result of one of its engineers failing to update Plex on their home computer and hackers exploiting a vulnerability (The patch to prevent this was deployed in May 2020)

LastPass suffered two large-scale and public data breaches last year. Information from the first breach was used to carry out the second attack, and a keylogger was installed on a senior DevOp's engineer's home computer, which was key to the success of the November attack.

LastPass revealed the hacker pulled off the breach by installing malware on an employee's home computer, by compromising a Plex media server, enabling them to capture keystrokes on the machine; This attack captured the employee's master password to their LastPass corporate vault.



# Wrapping up:

- InfoStealer malware is rampant
- You are a target
- Don't click links you don't recognize and be careful where you save an input your credentials
- Use unique passwords
- Regularly patch your applications and OS
- Keep personal and corporate access separate



*Don't try it.*

**!! CYB: Don't go to sites listed in this presentation or attempt to purposely involve yourself in the world of ISM !!**





# Questions?

Please take a moment to let us know how we did!

<https://www.menti.com/bldwfjbungjz>

Or <https://www.menti.com> with voting code

**9909 3092**



# M&T Tech



M&T Tech