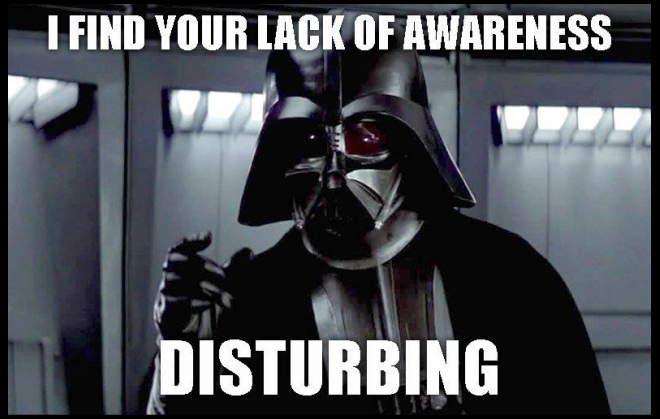
The Silent Thief:

Exploring the Dangers of Info Stealer Malware

Taylor Kaufman, Advanced Threat Hunter



M&T Tech

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

M&T Tech

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)**

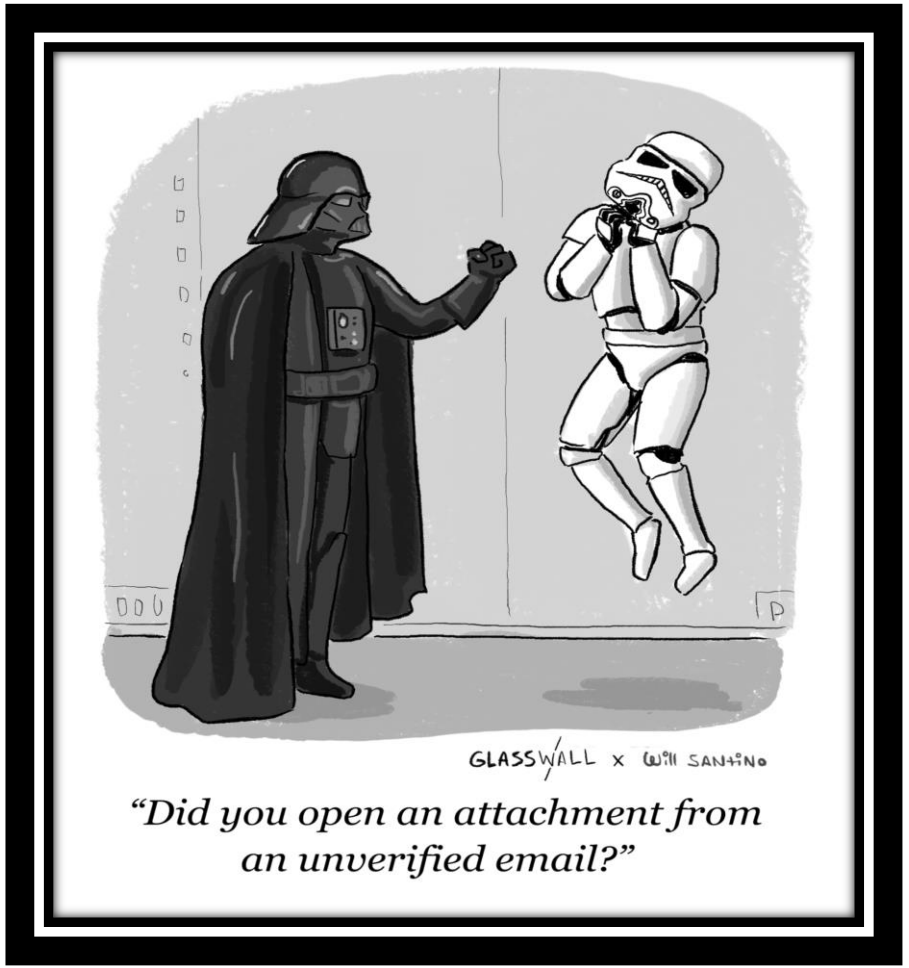
M&T Tech

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



M&T Tech

What is Stealer Malware After?

- 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

M&T Tech

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

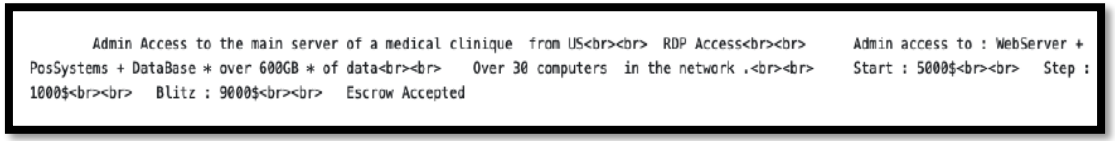
- Use your accounts to distribute more malware

M&T Tech

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



M&T Tech

How does InfoStealer malware work?

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

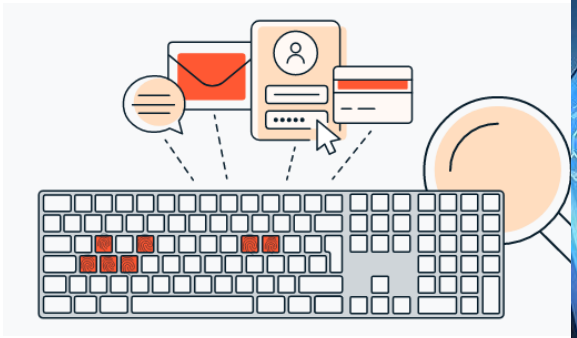
Info stealers may use many methods of data acquisition such as:

- 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

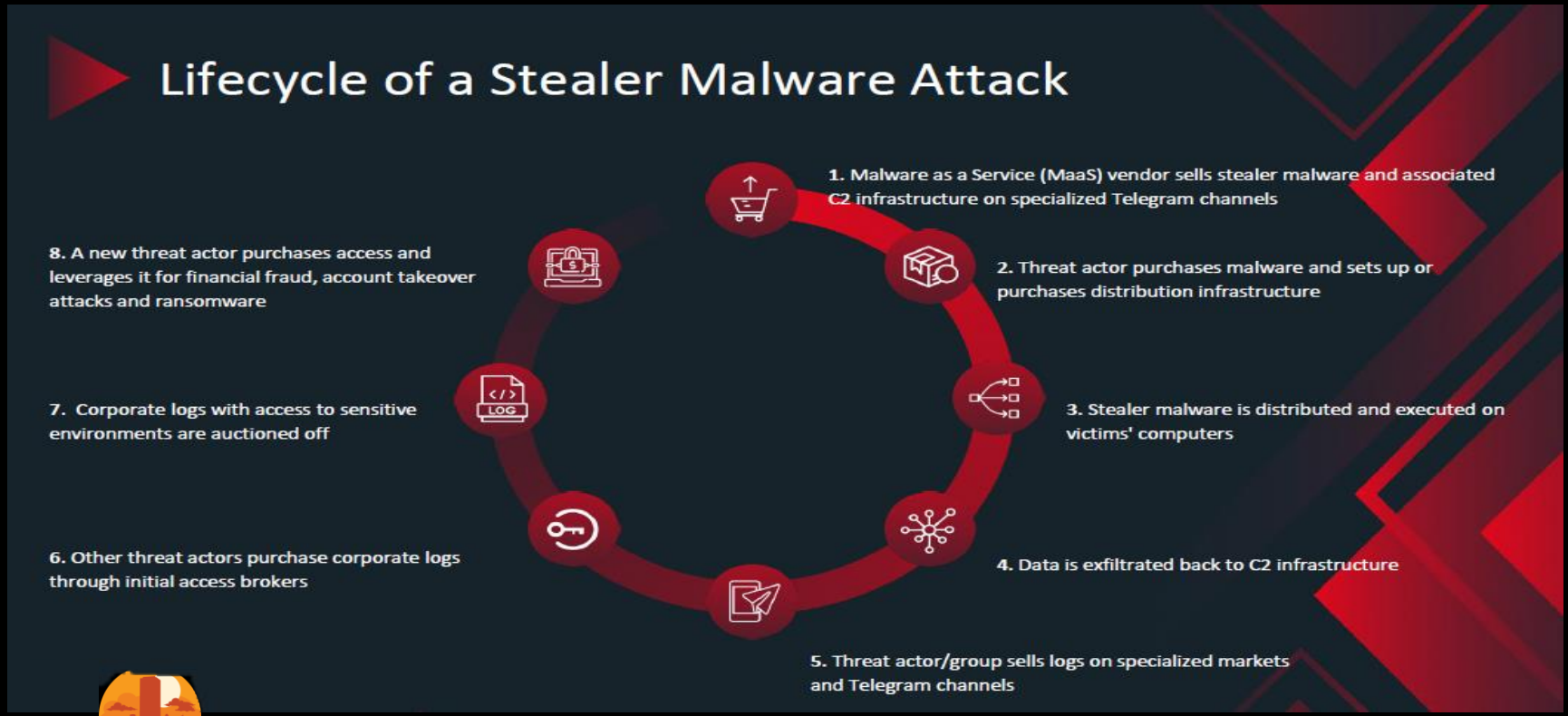
What constitutes the ISM makeup?

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
1. Malware as a Service (MaaS) vendor sells stealer malware and associated C2 infrastructure on specialized Telegram channels
2. Threat actor purchases malware and sets up or purchases distribution infrastructure
3. Stealer malware is distributed and executed on victims' computers
4. Data is exfiltrated back to C2 infrastructure
5. Threat actor/group sells logs on specialized markets and Telegram channels
6. Other threat actors purchase corporate logs through initial access brokers
7. Corporate logs with access to sensitive environments are auctioned off
8. A new threat actor purchases access and leverages it for financial fraud, account takeover attacks and ransomware
LOG

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

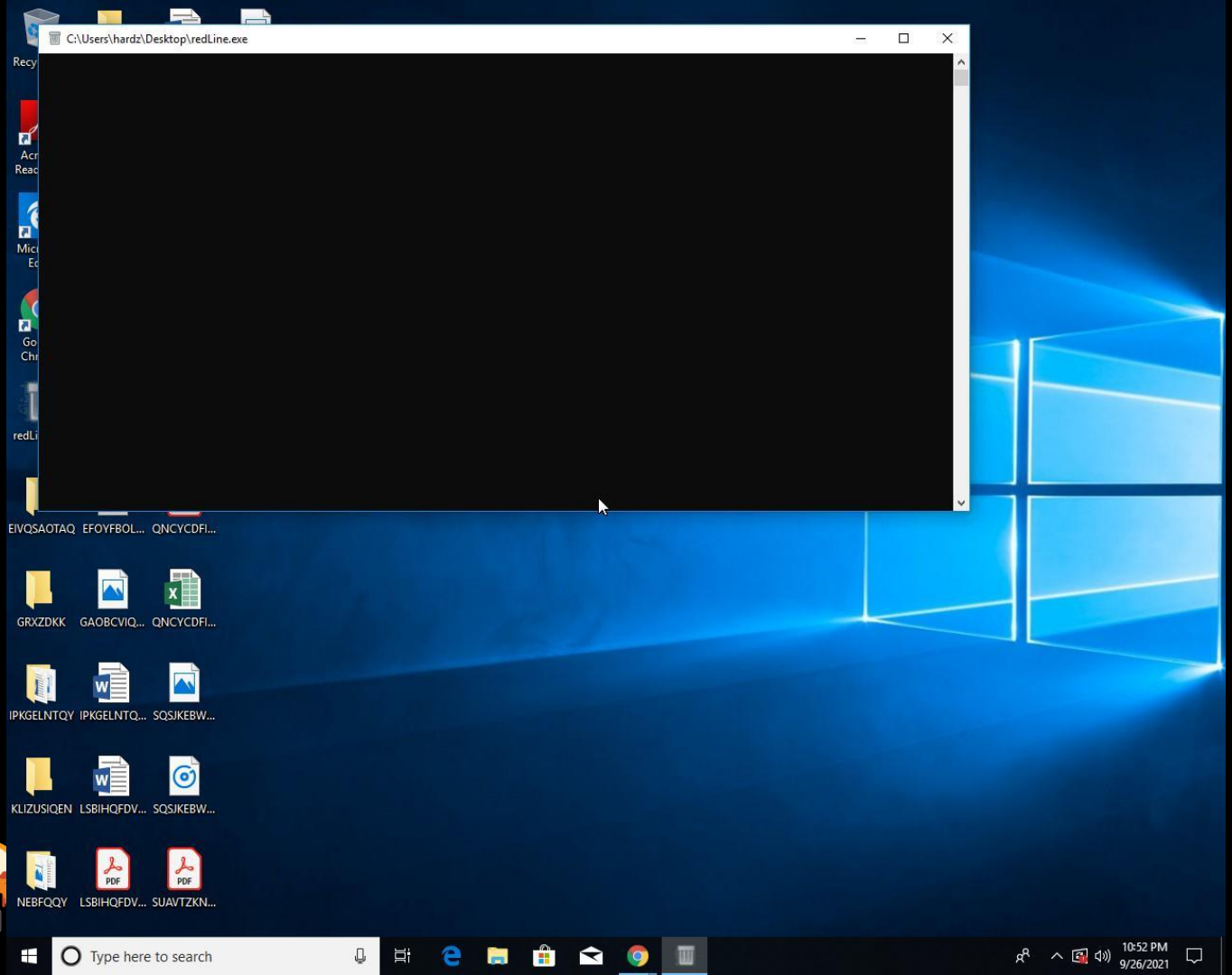
6. Additional modules are remotely downloaded from C2 infrastructure

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


Recycle Bin
NVWZAP...
NEBFQQY...
ZQIXMVQ...
Acrobat Reader DC
PWCCAW...
NEBFQQY...
ZQIXMVQ...
Excel 2016
Word 2016
Microsoft Edge
QCFWYSK
PIVFAGEAA...
Google Chrome
ZQIXMVQ
PWCCAW...
redLine.exe
DUUDTUB...
QNCYCDFI...
EIVQSAOTAQ
EFOYFBOL...
QNCYCDFI...
GRXZDKK
GAOBCVIQ...
QNCYCDFI...
IPKGELNTQY
IPKGELNTQ...
SQSJKEBW...
KLIZUSIQEN
LSBIHQFDV...
SQSJKEBW...
NEBFQQY
LSBIHQFDV...
SUAVTZKN...
Type here to search
10:54 PM
9/26/2021


C:\Users\hardz\Desktop\redLine.exe
Recy
Acr
Read
Mic
Ed
Go
Chr
redLi
EIVQSAOTAQ
EFOYFBOL...
QNCYCDFI...
GRXZDKK
GAOBCVIQ...
QNCYCDFI...
IPKGELNTQY
IPKGELNTQ...
SQSJKEBW...
KLIZUSIQEN
LSBIHQFDV...
SQSJKEBW...
NEBFQQY
LSBIHQFDV...
SUAVTZKN...
Type here to search
10:52 PM
9/26/2021


Recycle Bin
NVWZAP...
NEBFQQY...
ZQIXMVQ...
Acrobat Reader DC
PWCCAW...
NEBFQQY...
ZQIXMVQ...
Excel 2016
Word 2016
Microsoft Edge
QCFWYSK
PIVFAGEAA...
Google Chrome
ZQIXMVQ
PWCCAW...
redLine.exe
DUUDTUB...
QNCYCDFI...
EIVQSAOTAQ
EFOYFBOL...
QNCYCDFI...
GRXZDKK
GAOBCVIQ...
QNCYCDFI...
IPKGELNTQY
IPKGELNTQ...
SQSJKEBW...
KLIZUSIQEN
LSBIHQFDV...
SQSJKEBW...
NEBFQQY
LSBIHQFDV...
SUAVTZKN...
Type here to search
10:54 PM
9/26/2021

General Information

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

Most interesting Screenshot:

Detection

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

SEVEN ONE TECH

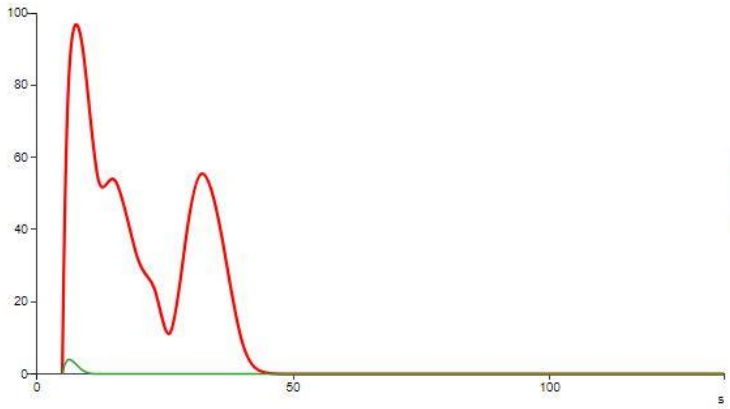
M&T Tech

IPs

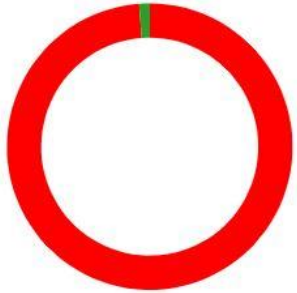
Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.9.20.20	iT1f2b2uQG.exe	Get hash	malicious	Browse	
	4by0i2GYt1.exe	Get hash	malicious	Browse	
	xfCwGNck6H.exe	Get hash	malicious	Browse	
	ec0d0t6b46.exe	Get hash	malicious	Browse	
	aG1d7FdZey.exe	Get hash	malicious	Browse	
	VnKKRx4E3c.exe	Get hash	malicious	Browse	
	MAauX39db3.exe	Get hash	malicious	Browse	
	p2r5ojd3Ec.exe	Get hash	malicious	Browse	
	OmIEwqzYLr.exe	Get hash	malicious	Browse	
	ae48GWjkLE.exe	Get hash	malicious	Browse	
	VhikmSr52Q.exe	Get hash	malicious	Browse	
	SLISRI5MIB.exe	Get hash	malicious	Browse	
	vc9TwhTemB.exe	Get hash	malicious	Browse	
	h28sBGvX8o.exe	Get hash	malicious	Browse	
	8XoievJlmd.exe	Get hash	malicious	Browse	
	D7fedJj8na.exe	Get hash	malicious	Browse	
	IT0uVNcO30.exe	Get hash	malicious	Browse	
	CHMr3BVD15.exe	Get hash	malicious	Browse	
	2N7AR7Ltmb.exe	Get hash	malicious	Browse	
	hXyGaeSOy7.exe	Get hash	malicious	Browse	

M&T Tech

CPU Usage

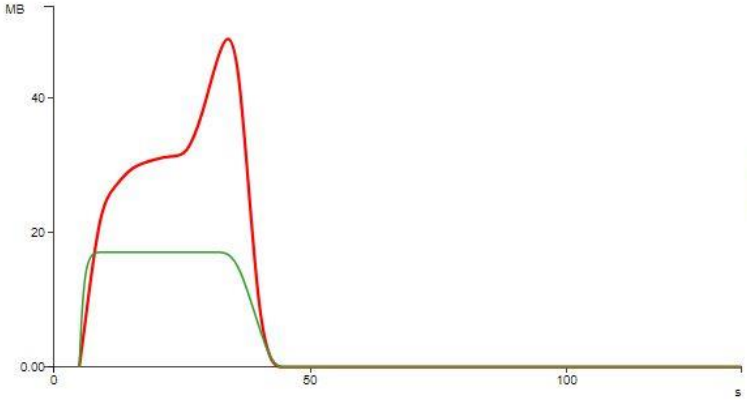


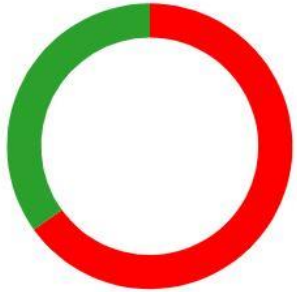
Click to jump to process



redLine.exe
conhost.exe

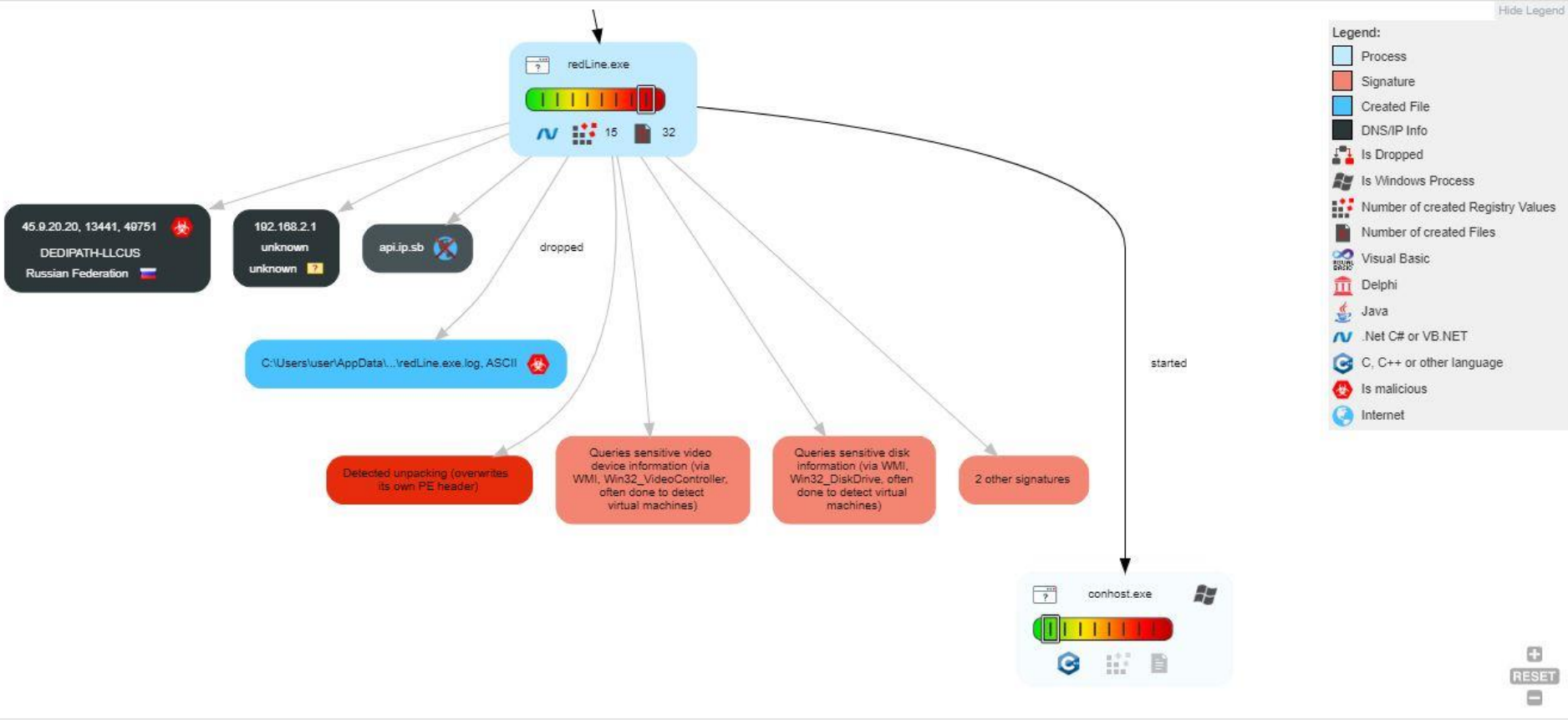
Memory Usage



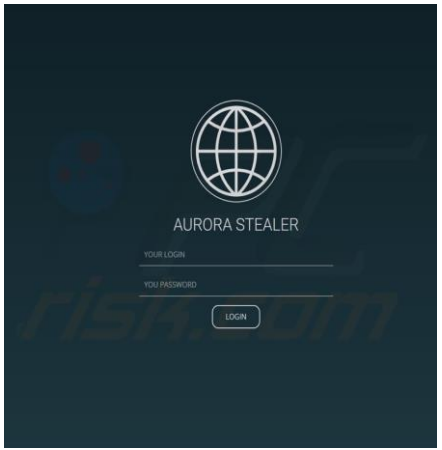


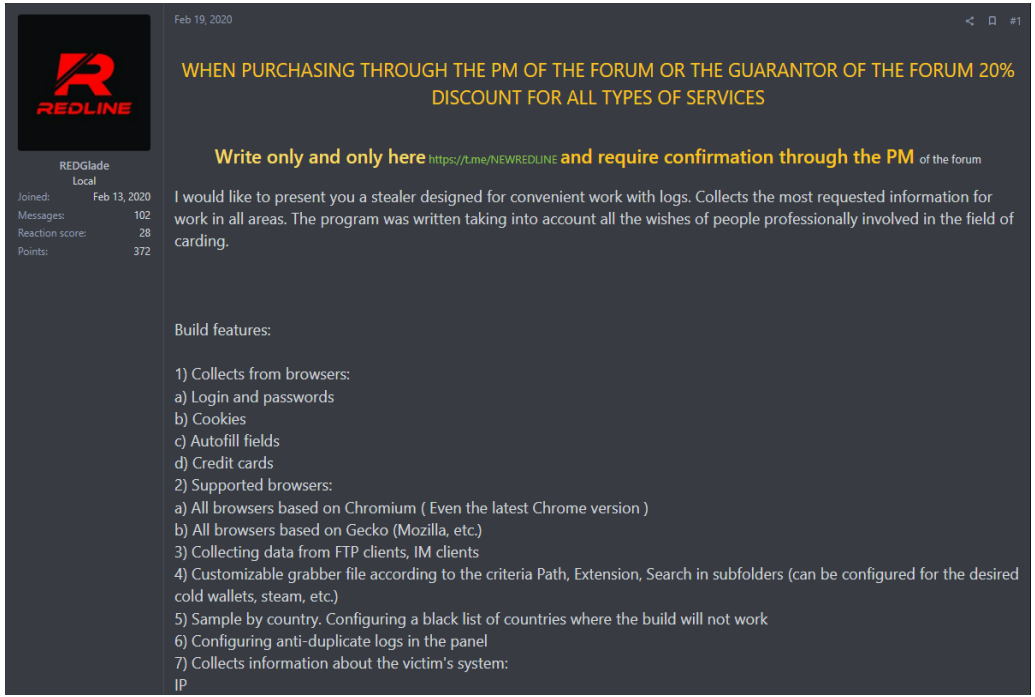
redLine.exe
conhost.exe

M&T Tech


redLine.exe
15
32
45.9.20.20, 13441, 49751
DEDIPATH-LLCUS
Russian Federation
192.168.2.1
unknown
unknown
api.ip.sb
dropped
C:\Users\user\AppData\...\redLine.exe.log, ASCII
started
Detected unpacking (overwrites its own PE header)
Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)
2 other signatures
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
RESET

The Main Families*

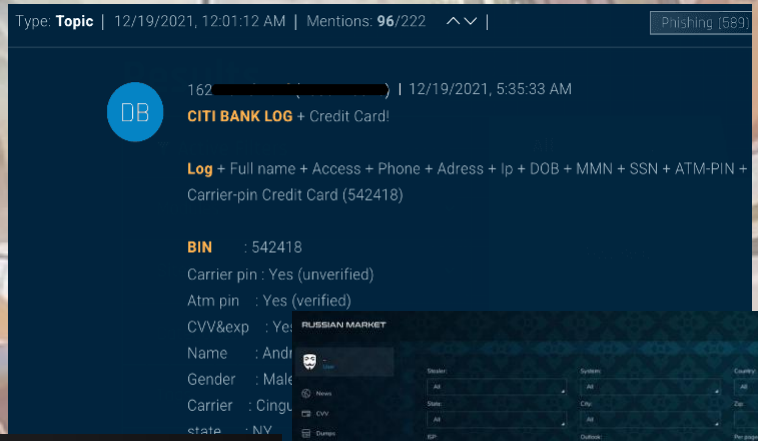


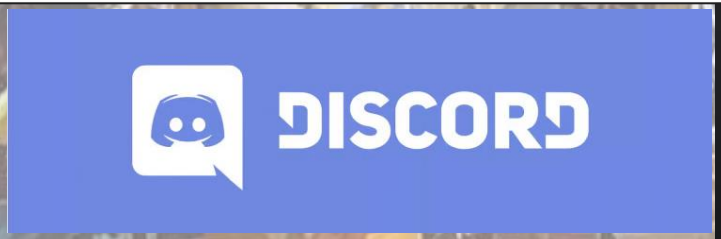


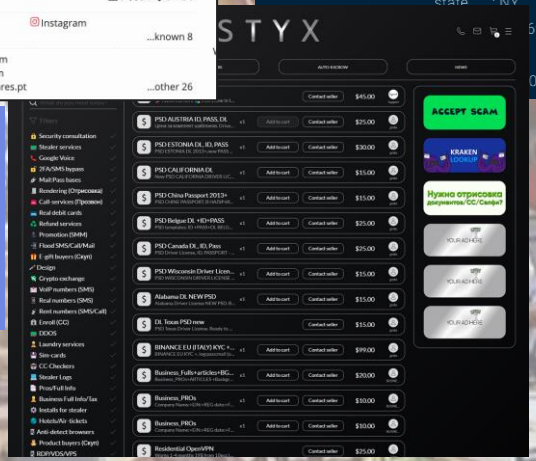
*Not an all-encompassing list

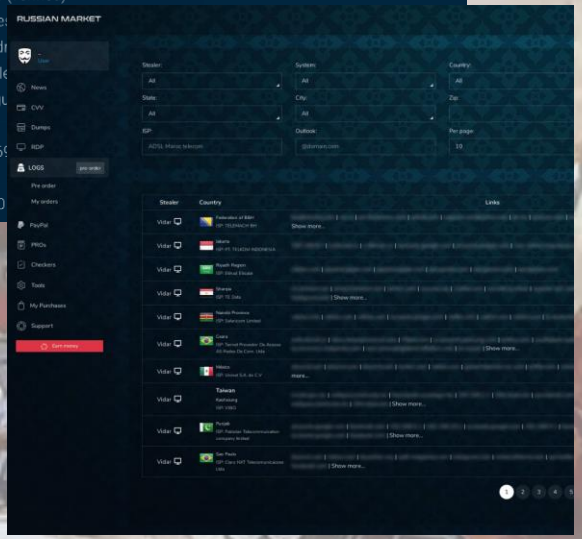
M&T Tech

The Trader Outposts of Stolen Information









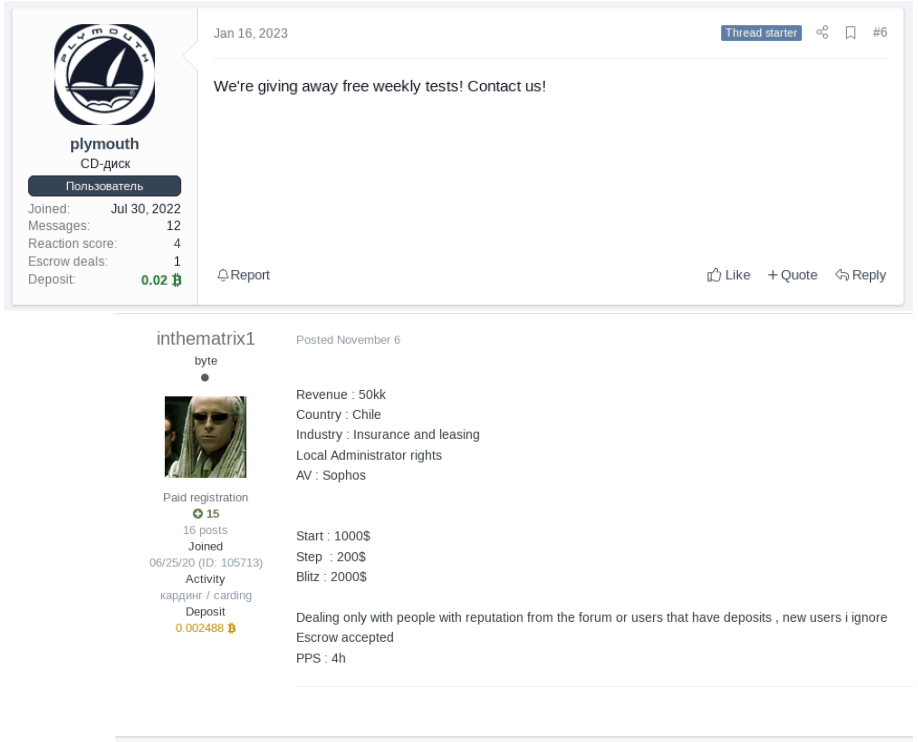
M&T Tech

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)

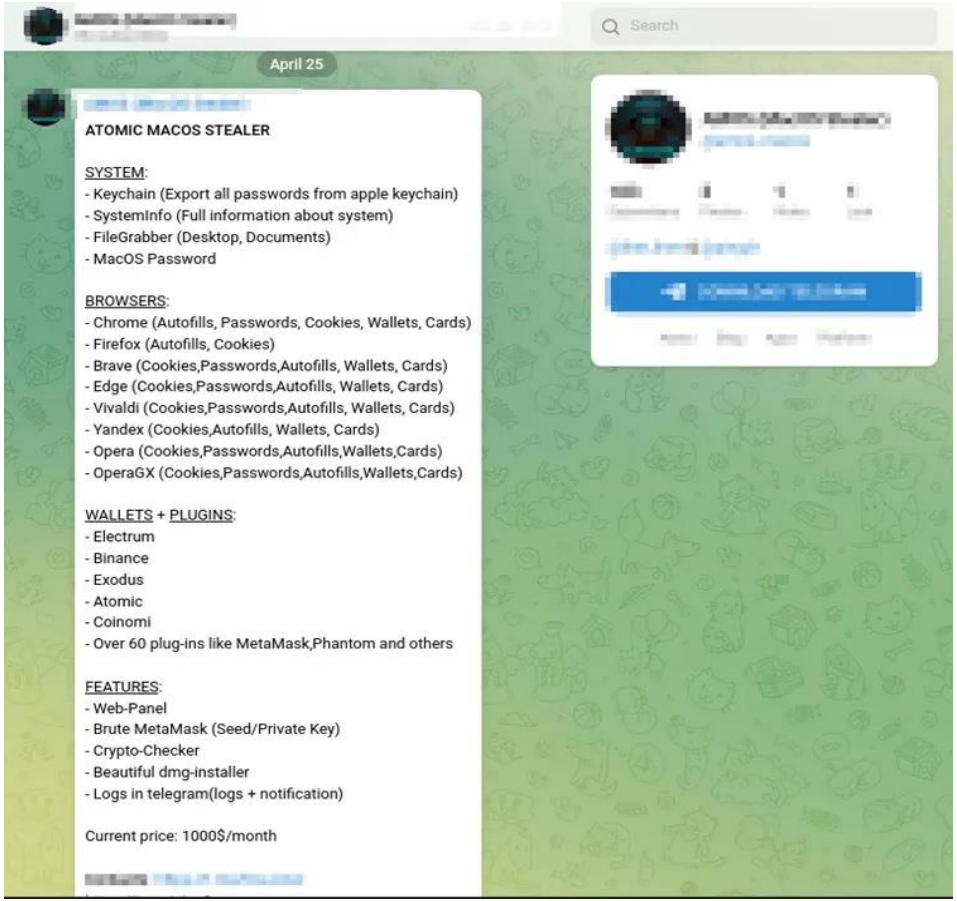


M&T Tech

“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.



M&T Tech

Why is this such a profitable industry?

And why hasn't anyone stopped this yet??

[redacted]
|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 ⭕
|Wire : Unknown ⭕
|IDentity : Driver's license
|Proof : [redacted]
|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 $
[redacted]
> 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

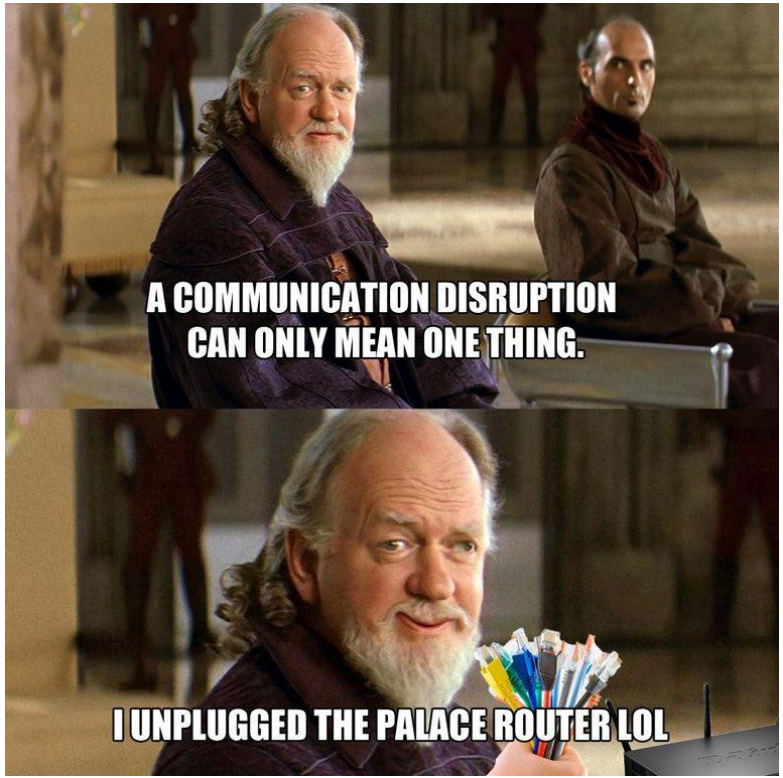
Work/M&T Bank accounts

- 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) 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

M&T Tech

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



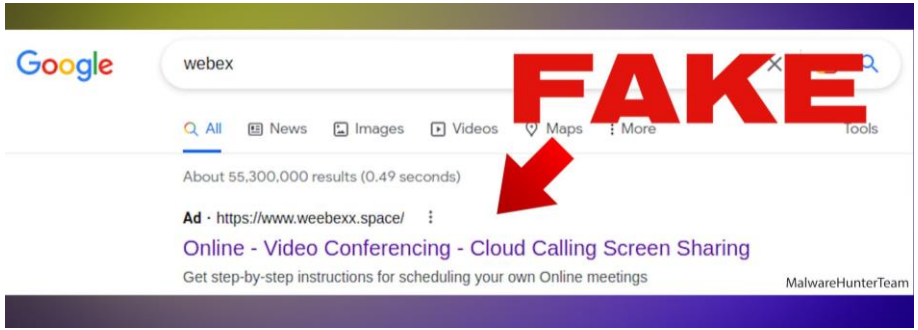
M&T Tech

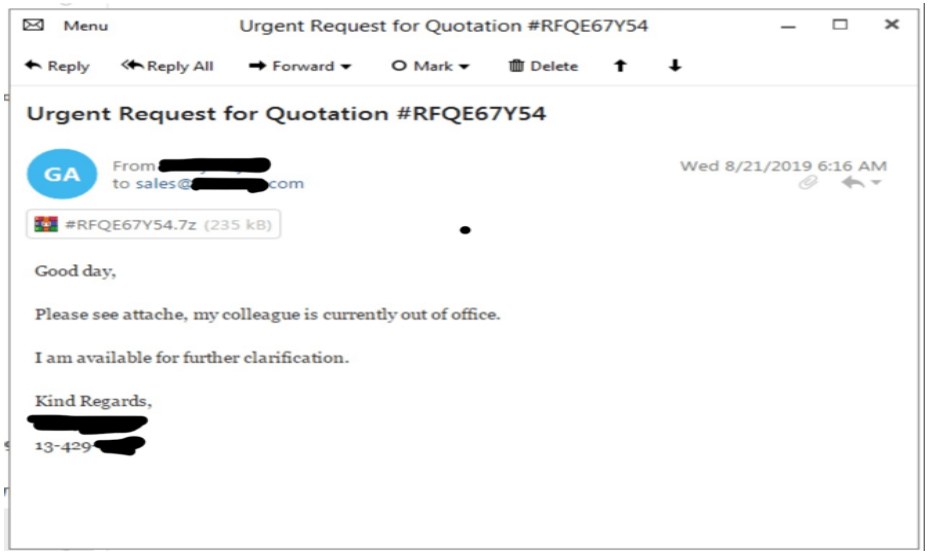
What is M&T doing to prevent InfoStealer infections?

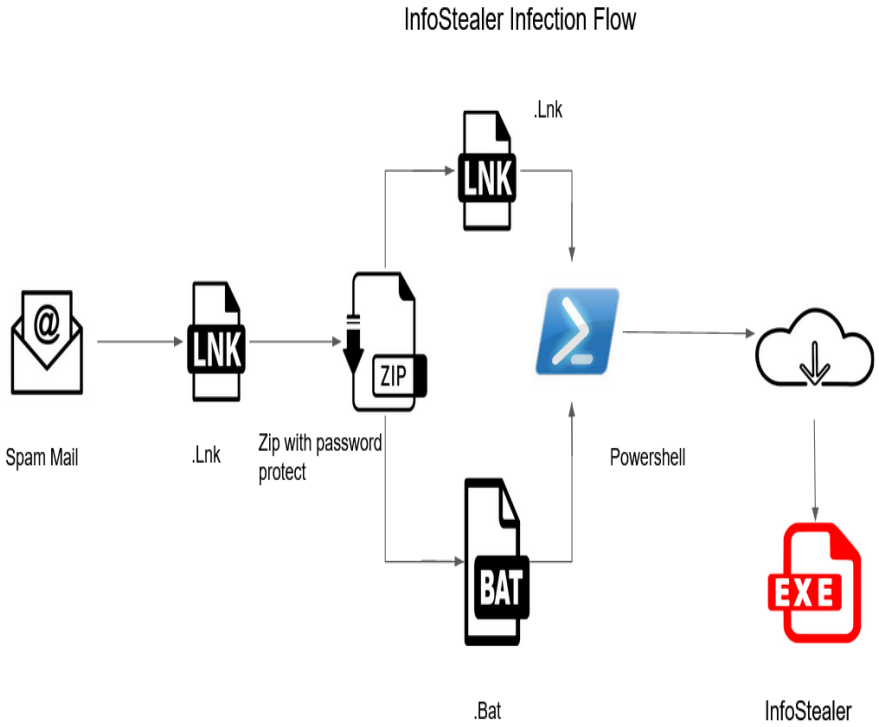
- Threat Intel monitoring for stolen credentials (both customers and employees)
- CSOC alert monitoring for unusual logins and malicious downloads
- Phishing email monitoring and protections (both report mailbox and vendor provided intel/response)
- Threat Hunting on new techniques and campaigns
- Vulnerability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

M&T Tech

How to recognize InfoStealer







M&T Tech

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.

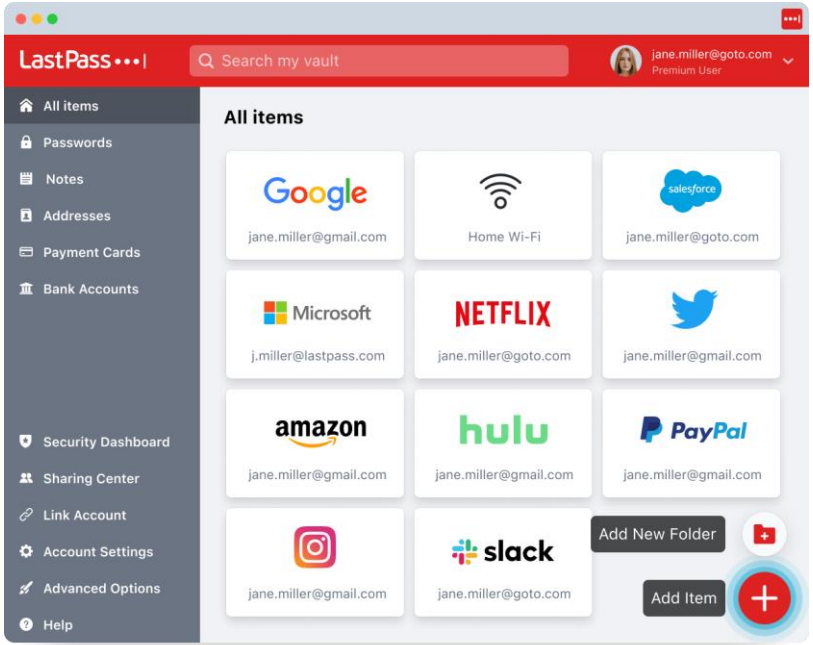
“Someone on the Linus Media Group’s team downloaded “what appeared to be a sponsorship offer from a potential partner” and launched the included PDF with the terms of that offer.
This offer actually contained malware that accessed “all user data from both their installed browsers” — including session 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.



M&T Tech

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

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

M&T Tech

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