F-Secure

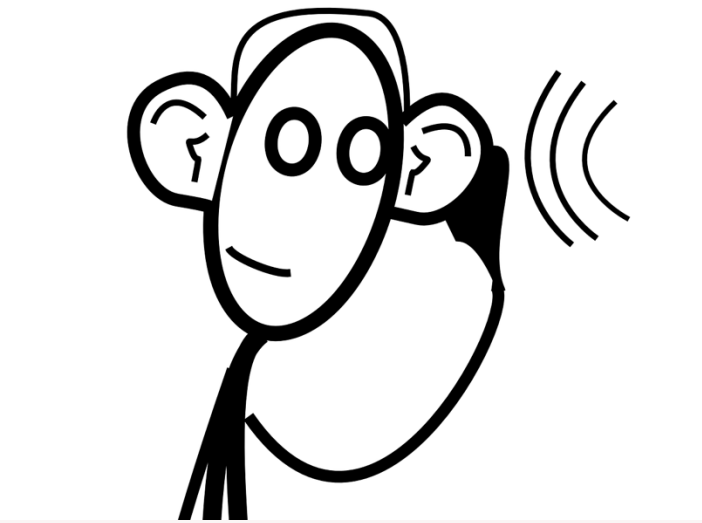
From Prey to Playbook

Using Infostealer Logs to Understand Victim Behavior

Dr. Megan Squire

DEFCON 33 | Red Team Village Workshop

Having trouble hearing this talk?



Loud room + no mic = hard to hear

I posted my talk & speaker notes at

https://github.com/megansquire/syntheticInfostealers

whoami

Currently:

- Threat Intelligence Researcher, F-Secure

Previously:

- Deputy Dir. for Data Analytics & OSINT, Southern Poverty Law Center
- Professor of Computer Science, Elon University

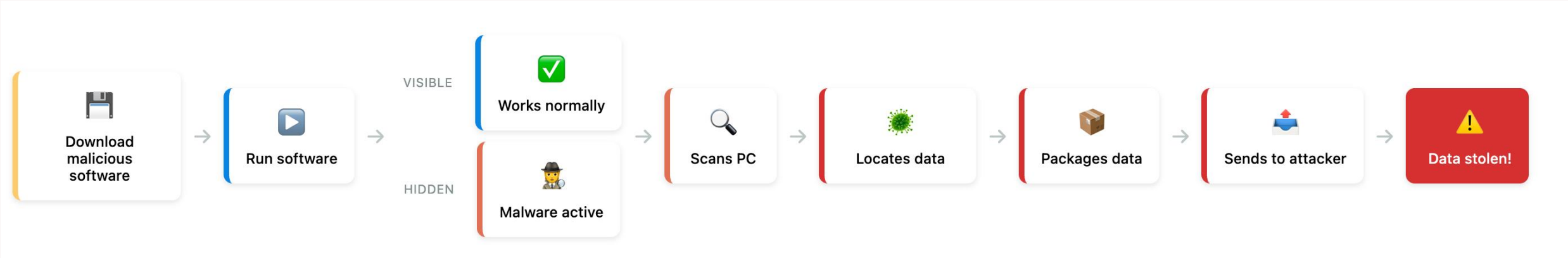
https://www.linkedin.com/in/megansquire

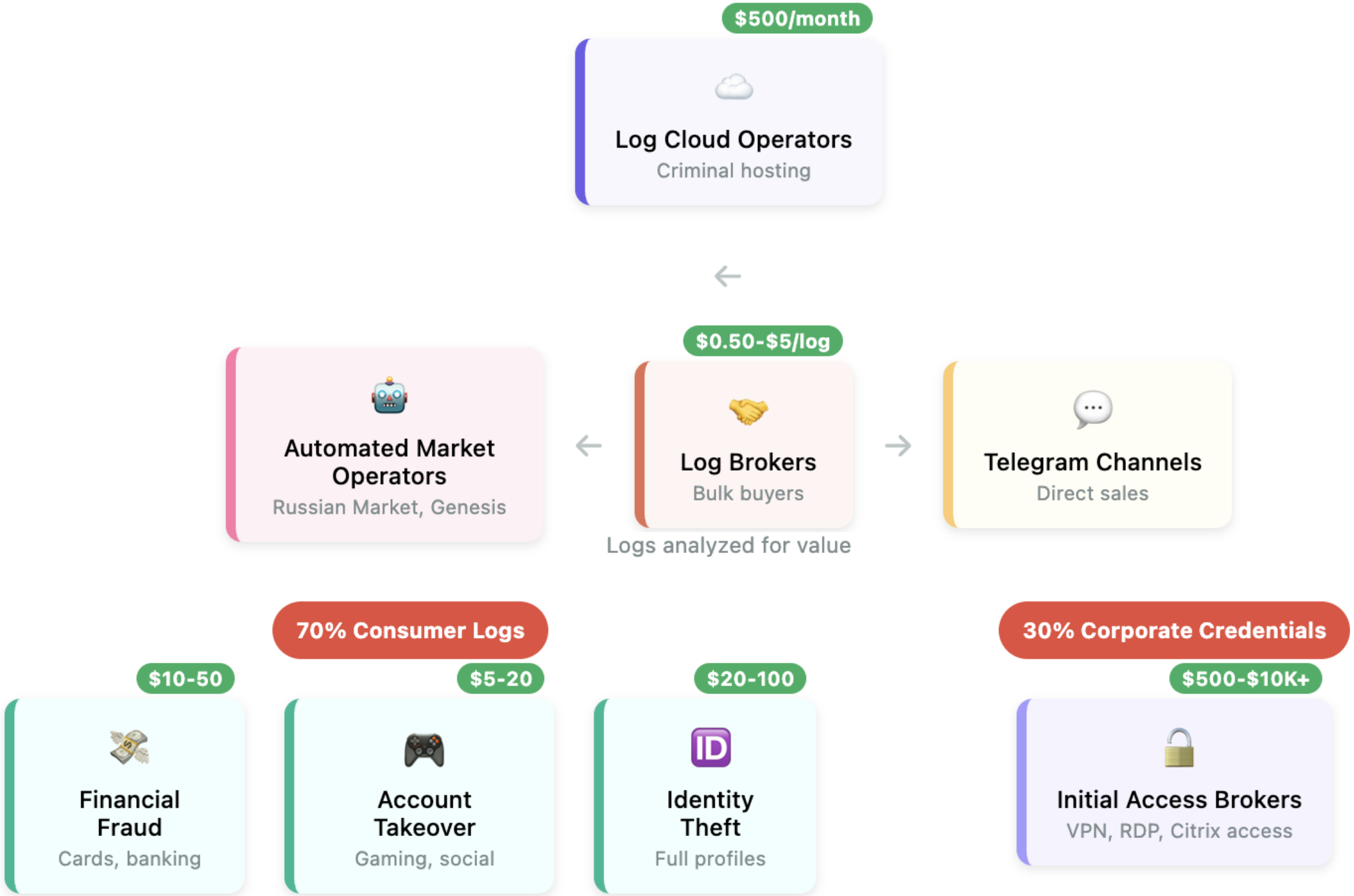
Workshop Outline

1. Overview of Infostealers
2. Research Questions
3. Synthetic Data
4. Dupes and Fakes
5. A Red-Teaming Protocol
6. Working with the Protocol

What is an infostealer?

The infection process




$500/month
Log Cloud Operators
Criminal hosting
$0.50-$5/log
Automated Market Operators
Russian Market, Genesis
Log Brokers
Bulk buyers
Telegram Channels
Direct sales
Logs analyzed for value
70% Consumer Logs
30% Corporate Credentials
$10-50
Financial Fraud
Cards, banking
$5-20
Account Takeover
Gaming, social
$20-100
Identity Theft
Full profiles
$500-$10K+
Initial Access Brokers
VPN, RDP, Citrix access

Infostealers, by the numbers

How big is this problem?

10,000	183	2.1 billion
Victims per day	Countries	Stolen credentials (2024)

38% increase over 2023

66% of all stolen credentials come from infostealers

Families

Some of the more common infostealer families

Lumma
Redline
Atomic Mac Stealer
StealC
Vidar
Raccoon
Blackguard
Jester
Xehook
Meduza

Cryptbot
Banshee
Phemedrome
Luca
Blankgrabber
Astris
Risepro
Stealerium
Noxy
DarkCrystal

Elusive
AZORult
Rhadamanthys
Rusty
Fickle
Luca
Predator
Ailurophile
Arech Client
RL Stealer

And so many more…

Recognizing infostealers

Tips and tricks

Sometimes the stealer makes it really obvious which one it is:

```
-- VIDAR STEALER - ЛУЧШИЙ STEALER НА РЫНКЕ!!!!
-- Контакты для связи Telegram: @vidar
-- ПОМНИТЕ ОПЛАТА ТОЛЬКО НА САЙТЕ ПРОЕКТА В АВТОМАТИЧЕСКОМ РЕЖИМЕ!

Chat Public: https://t.me/vidarchatopen
Channel: https://t.me/vidarnews
```

```
***********************************************
*                                             *
*   ____  _____ ____  _     ___ _   _ _____   *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____|  *
*  | |_) |  _| | | | | |    | ||  \| |  _|    *
*  |  _ <| |___| |_| | |___ | || |\  | |___   *
*  |_| \_|_____|____/|_____|___|_| \_|_____|  *
*                                             *
*  Telegram: https://t.me/redline_market_bot  *
***********************************************
```

Recognizing infostealers

Tips and tricks

Sometimes you might need to look closer into the log's "header" file.

This is a really good resource for learning more about the different stealer families:

https://github.com/MalBeacon/what-is-this-stealer

They have YARA rules for recognizing the header files based on how they are laid out.

Examples of header files

A few samples

What stealer is this?

```
# Buy now: TG @lummanowork
# Buy&Sell logs: @lummamarketplace_bot
- LummaC2 Build: Nov 15 2024
- LID: hRjzG3--GUNNAR
- Configuration: 1fdd6cf0cfc18336b64c017c6c3650de
- Path: C:\WINDOWS\SysWOW64\msiexec.exe

- OS Version: Windows 10 Pro (10.0.19045) x64
- Local Date: 30.07.2025 13:19:25
- Time Zone: (UTC+00:00) UTC
- Install Date: 24.02.2024 13:19:25
- Elevated: false
- Computer: DESKTOP-30E4BCCF
- User: diego
- Domain:
- Hostname: DESKTOP-30E4BCCF
- NetBIOS: DESKTOP-30E4BCCF
- Language: en-US
- Anti Virus:
    - Windows_Defender
- HWID: KV3G8KHY2E6YGKXW
- RAM Size: 8192MB
- CPU Vendor: GenuineIntel
- CPU Name: Intel(R) Core(TM) i5-10400 @ 2.90GHz
- CPU Threads: 8
- CPU Cores: 4
- GPU: NVIDIA GeForce GTX 1060 3GB
- Display resolution: 1366x768

- IP Address: 209.133.9.128
- Time: 30.07.2025 13:19:25 (sig:1753895965.ebcf74b00dc0486feed4eb5ff7f881bd)
- Country: MX

------------------------------------

Automated log store >> t.me/lummamarketbot
Tens of thousands of logs for sale, rating system, search by filters and countries, hundreds of sellers
Purchase quality material right now - t.me/lummamarketbot
```

```
# Buy now: TG @lummanowork
# Buy&Sell logs: @lummamarketplace_bot
- LummaC2 Build: Nov 15 2024
- LID: hRjzG3--GUNNAR
- Configuration: 1fdd6cf0cfc18336b64c017c6c3650de
- Path: C:\WINDOWS\SysWOW64\msiexec.exe

- OS Version: Windows 10 Pro (10.0.19045) x64
- Local Date: 30.07.2025 13:19:25
- Time Zone: (UTC+00:00) UTC
- Install Date: 24.02.2024 13:19:25
- Elevated: false
- Computer: DESKTOP-30E4BCCF
- User: diego
- Domain:
- Hostname: DESKTOP-30E4BCCF
- NetBIOS: DESKTOP-30E4BCCF
- Language: en-US
- Anti Virus:
    - Windows_Defender
- HWID: KV3G8KHY2E6YGKXW
- RAM Size: 8192MB
- CPU Vendor: GenuineIntel
- CPU Name: Intel(R) Core(TM) i5-10400 @ 2.90GHz
- CPU Threads: 8
- CPU Cores: 4
- GPU: NVIDIA GeForce GTX 1060 3GB
- Display resolution: 1366x768

- IP Address: 209.133.9.128
- Time: 30.07.2025 13:19:25 (sig:1753895965.ebcf74b00dc0486feed4eb5ff7f881bd)
- Country: MX

-----------------------------------

Automated log store >> t.me/lummamarketbot
Tens of thousands of logs for sale, rating system, search by filters and countries, hundreds of sellers
Purchase quality material right now - t.me/lummamarketbot
```

Lumma (System.txt)

```
- LummaC2 Build: Oct 21 2024
- LID: 4SD0y4--MAGISTER
- Configuration:
- Path: C:\Users\pc\AppData\Local\Temp\1F58.exe

- OS Version: Windows 11 Pro (10.0.22631) x64
- Local Date: 26.10.2024 19:00:18
- Time Zone: UTC+4
- Install Date: 23.02.2024 11:01:58
- Elevated: false
- Computer:DESKTOP-5ABF2TC
- User: pc
- Domain:
- Hostname: DESKTOP-5ABF2TC
- NetBIOS: DESKTOP-5ABF2TC
- Language: ar-AE
- Anti Virus:
    - Windows Defender
- HWID: 2FC5E1B5B129FD4CDB71E32F12995CB3
- RAM Size: 16384MB
- CPU Vendor: GenuineIntel
- CPU Name: 11th Gen Intel(R) Core(TM) i5-11400F @ 2.60GHz
- CPU Threads: 12
- CPU Cores: 6
- GPU: NVIDIA GeForce RTX 3050
- Display resolution: 1920x1080

- IP Address: 127.0.0.1
- Time: 26.10.2024 18:00:17 (sig:1729954817.083b646b6e3d8a67d
- Country: AE
```

Examples of header files

A few samples

What stealer is this?

```
CLOUD LOGS - @FATECLOUD | SHOP - @LOGSFATE_BOT | SUPPORT - @EZFATE

Build ID: @premium_logs
IP: 172.58.207.124
FileLocation: C:\Users\Amanda\AppData\Local\Temp\680199\flesh.exe
UserName: Amanda
MachineName: DESKTOP-69DSCPWV
Country: US
Zip Code: 62655
Location: Austin, Texas
HWID: C470995631EB50949A1486556DB55095
Current Language: English (United States)
ScreenSize: {Width=2560, Height=1440}
TimeZone: (UTC+00:00) Coordinated Universal Time
Operation System: Windows_11_Home x64
Log date: 7/29/2025 2:27:03 PM

Available KeyboardLayouts:
English (United States)


Hardwares:
Name: Total of RAM, 16384.00 Mb or 17179869184 bytes
Name: AMD Ryzen 5 5600X, 6 Cores
Name: Intel(R) UHD Graphics 730, 4294967296 bytes


Anti-Viruses:
Windows Defender
```

```
CLOUD LOGS - @FATECLOUD | SHOP - @LOGSFATE_BOT | SUPPORT - @EZFATE

Build ID: @premium_logs
IP: 172.58.207.124
FileLocation: C:\Users\Amanda\AppData\Local\Temp\680199\flesh.exe
UserName: Amanda
MachineName: DESKTOP-69DSCPWV
Country: US
Zip Code: 62655
Location: Austin, Texas
HWID: C470995631EB50949A1486556DB55095
Current Language: English (United States)
ScreenSize: {Width=2560, Height=1440}
TimeZone: (UTC+00:00) Coordinated Universal Time
Operation System: Windows_11_Home x64
Log date: 7/29/2025 2:27:03 PM

Available KeyboardLayouts:
English (United States)


Hardwares:
Name: Total of RAM, 16384.00 Mb or 17179869184 bytes
Name: AMD Ryzen 5 5600X, 6 Cores
Name: Intel(R) UHD Graphics 730, 4294967296 bytes


Anti-Viruses:
Windows Defender
```

RedLine/META (UserInformation.txt)

```
Build ID: TG
IP: 127.0.0.1
FileLocation: C:\Users\Soliman\AppData\Roaming\LqKC6wx1X7.exe
UserName: John
MachineName: DESKTOP-I5DF3AA
Country: AE
Zip Code: UNKNOWN
Location: Dubai, Dubayy
HWID: 122C51E4AF1735E9123E2A94C1AC26A0D
Current Language: English (United States)
ScreenSize: {Width=1536, Height=864}
TimeZone: (UTC+04:00) Abu Dhabi, Muscat
Operation System: Windows 10 Pro x64
Log date: 7/4/2024 5:43:07 PM

Available KeyboardLayouts:
English (United Kingdom)
English (United States)
Arabic (Egypt)


Hardwares:
Name: Total of RAM, 8087.34 Mb or 8480190464 bytes
Name: Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 2 Cores
Name: Intel(R) HD Graphics 520, 1073741824 bytes


Anti-Viruses:
Windows Defender
```

What else is in the logs?

Each infostealer stores information slightly differently

- Autofill
- cookie_list.txt
- Cookies
- Downloads
- information.txt
- passwords.txt
- screenshot.jpg

Vidar

- All Passwords.txt
- Brute.txt
- Chrome
- Clipboard.txt
- Cookies
- Firefox
- Processes.txt
- Screen.png
- Software.txt
- System.txt

Lumma

- Autofills
- Cookies
- DomainDetects.txt
- ImportantAutofills.txt
- InstalledBrowsers.txt
- InstalledSoftware.txt
- Passwords.txt
- ProcessList.txt
- Restore
- Screenshot.jpg
- Telegram
- UserAgents
- UserInformation.txt
- Wallets

Redline

Research questions

Red Teaming

How can we use infostealers as a data source for red teaming?

Victim Behavior

What can we learn about victim/target behavior from studying infostealers?

Practicalities

What are some practical techniques for efficiently working with this data?

Practicalities

Some tips for working with infostealer data

Where to get infostealer logs

Build

- Collect files yourself
- Create synthetic files

Buy

- Find a vendor

When working with this kind of data, be aware of the relevant laws in your area, and always stay within your rules of engagement.

I made synthetic logs for this talk

Why?

- So I could show you tons of examples of logs but without showing real people’s data.
- I also thought it might be interesting to have a mechanism for creating millions of believable but fake infostealers. 🤔

Synthetic logs – my process

1. Choose five families to focus on
    1. Atomic
    2. Lumma
    3. Redline
    4. Stealc
    5. Vidar
2. Collect real samples from these families
3. Extract the salient features of each family
    - What files do they create?
    - What fields are in each file?
    - How are the files formatted?
4. Write code to generate fake log files following these features

Synthetic logs – persona creation

	A	B	C	D	E	F	G	H	I	J	K	L
1	Infection	PersonaID	FirstName	LastName	Age	Occupation	IncomeLevel	Country	State_Regio	City	Timezone	PrimaryLang
2	Stealc	P001	Sarah	Moonbeam	34	Marketing Mana	Medium	US	Oregon	Portland	UTC-8	English
3	Lumma	P002	Michael	Glitter	28	Software Develo	High	US	California	San Francisco	UTC-8	English
4	Redline	P003	Amanda	Butterfly	31	UX Designer	Medium	US	Texas	Austin	UTC-6	English
5	Redline	P004	David	Telescope	29	Data Analyst	Medium	US	Washington	Seattle	UTC-8	English
6	Redline	P005	Jessica	Rainbow	33	Project Manager	Medium	US	Colorado	Denver	UTC-7	English
7	Stealc	P006	Robert	Elephant	41	Sales Director	High	US	Illinois	Chicago	UTC-6	English
8	Redline	P007	Lisa	Kangaroo	27	Content Writer	Low	US	North Carolina	Raleigh	UTC-5	English
9	Lumma	P008	Kevin	Slipper	35	Cybersecurity Ar	High	US	Virginia	Richmond	UTC-5	English
10	Stealc	P009	Maria	Horsefeather	30	HR Manager	Medium	US	Florida	Tampa	UTC-5	Spanish
11	Vidar	P010	James	Sparkle	38	Operations Mana	Medium	US	Georgia	Atlanta	UTC-5	English
12	Lumma	P011	Lukas	Pineapple	26	Graphic Designe	Low	DE	Bavaria	Munich	UTC+1	German
13	Vidar	P012	João	Sandwich	32	Software Engine	Medium	BR	São Paulo	São Paulo	UTC-3	Portuguese
14	Stealc	P013	Anastasia	Muffin	29	Customer Succe	Medium	RU	Moscow	Moscow	UTC+3	Russian
15	Stealc	P014	Alejandro	Pickle	25	Junior Develope	Low	MX	Nuevo León	Monterrey	UTC-6	Spanish
16	Lumma	P015	Priya	Bubble	31	Business Analys	Medium	IN	Karnataka	Bangalore	UTC+5:30	English
17	Lumma	P016	Matteo	Tornado	40	IT Manager	High	IT	Lombardy	Milan	UTC+1	Italian
18	Lumma	P017	Sophie	Velcro	31	Digital Marketing	Medium	FR	Île-de-France	Paris	UTC+1	French
19	Redline	P018	Hiroshi	Pancake	33	Financial Analys	High	JP	Tokyo	Tokyo	UTC+9	Japanese
20	Redline	P019	Isabella	Marble	28	Product Manage	Medium	CL	Santiago Metrop	Santiago	UTC-3	Spanish
21	Redline	P020	Artem	Thunder	34	DevOps Enginee	High	UA	Kyiv	Kyiv	UTC+2	Ukrainian
22	Redline	P021	Tyler	Jellybean	19	College Student	Low	US	Texas	Dallas	UTC-6	English
23	Stealc	P022	Kai	Volcano	23	Game Develope	Medium	JP	Tokyo	Tokyo	UTC+9	Japanese
24	Lumma	P023	Viktor	Cupcake	27	IT Support	Medium	RU	Saint Petersburg	Saint Petersburg	UTC+3	Russian

Our first workshop task

Let’s take a look at the synthetic stealer logs I created

Go here:
https://github.com/megansquire/syntheticInfostealers

Key Differences b/t Synthetic Stealer Logs & Real Stealer logs

1. The people names, domains, and company names are obviously fake
2. The screenshots are fake
3. Steam tokens just say [493 character token]
4. Not as much variety in the headers, ASCII art, etc
5. etc

A brief interlude

Dealing with FAKE and DUPLICATE data

A word about dupes and fakes

With real infostealer logs, you will likely run into a lot of duplicate logs and a lot of fake data

Many infostealer alert services and vendors will have duplicates in their systems.

```
# Buy now: TG @lummanowork
# Buy&Sell logs: @lummamarketbot
- LummaC2 Build: Dec 16 2024
- LID: @arsenalstuffff/@tallogs--LiveTraffic
- Configuration: 5c9b8674a630d9101b46733aa37f15ec
- Path: C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe
- OS Version: Windows 10 Pro (10.0.19041) x64
- Local Date: 22.12.2024 02:22:53
- Time Zone: UTC-7
- Install Date: 04.09.2024 15:03:29
- Elevated: false
- Computer: DESKTOP-EBKBI17
- User: WIN 10 PRO
- Domain:
- Hostname: DESKTOP-EBKBI17
- NetBIOS: DESKTOP-EBKBI17
- Language: en-US
- Anti Virus:
    - Windows Defender
- HWID: C4916E5A97EAE2ACA190C26FF9FF19FE
- RAM Size: 8192MB
- CPU Vendor: GenuineIntel
- CPU Name: Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
- CPU Threads: 4
- CPU Cores: 2
- GPU: Intel(R) HD Graphics 520
- Display resolution: 1920x1080
- IP Address: 103.120.117.120
- Time: 22.12.2024 12:23:13 (sig:1729235822.b6f5838d921aaeea7cb494df312a779d)
- Country: PK
-----------------------------------
Automated log store >> t.me/lummamarketbot
Tens of thousands of logs for sale, rating system, search by filters and countries,
Purchase quality material right now - t.me/lummamarketbot
```

```
CHANNEL:t.me/+iywVolQUH1swMzZi    ADMIN:t.me/capitan_blunt  CHAT:t.me/ErernityTeam

# Buy now: TG @lummanowork
# Buy&Sell logs: @lummamarketbot
- LummaC2 Build: Oct 15 2024
- LID: tLYMe5--222
- Configuration: 5c9b8674a630d9101b46733aa37f15ec
- Path: C:\Windows\BitLockerDiscoveryVolumeContents\BitLockerToGo.exe

- OS Version: Windows 10 Pro (10.0.19041) x64
- Local Date: 18.10.2024 00:16:57
- Time Zone: UTC-7
- Install Date: 04.09.2024 15:03:29
- Elevated: false
- Computer: DESKTOP-EBKBI17
- User: WIN 10 PRO
- Domain:
- Hostname: DESKTOP-EBKBI17
- NetBIOS: DESKTOP-EBKBI17
- Language: en-US
- Anti Virus:
    - Windows Defender
- HWID: C4916E5A97EAE2ACA190C26FF9FF19FE
- RAM Size: 8192MB
- CPU Vendor: GenuineIntel
- CPU Name: Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
- CPU Threads: 4
- CPU Cores: 2
- GPU: Intel(R) HD Graphics 520
- Display resolution: 1920x1080

- IP Address: 103.120.117.120
- Time: 18.10.2024 10:17:02 (sig:1729235822.b6f5838d921aaeea7cb494df312a779d)
- Country: PK
```

For dupes…

I found that clustering the logs according to similar sets of emails and domains worked pretty well.

1. Figure out the list of emails and domains in each log
2. Calculate a similarity matrix
3. Assign clusters
4. One cluster = one actual infection

This code is not on Github yet as it's sort of outside the scope of this talk, but I'll get it up there soon.

A word about fakes

You will find fake logs in both vendor databases and online in marketplaces.

For fakes, I found that there were two main “tells”:

1. High variability in the list of emails, domains, and usernames
   - Example: a log with 200 different email / password combos from 200 different companies and organizations

2. Header information that does not make sense

```
**********************************************
*                                            *
*   ____  _____ ____  _     ___ _   _ _____  *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____| *
*  | |_) |  _| | | | | |    | ||  \| |  _|   *
*  |  _ <| |___| |_| | |___ | || |\  | |___  *
*  |_| \_|_____|____/|_____|___|_| \_|_____| *
*                                            *
*  Telegram: https://t.me/redline_market_bot *
**********************************************

Build ID: mina
IP: 146.88.184.10
FileLocation: C:\Users\Flipper\Downloads\eP8yI6iOnxK83.exe
UserName: BCoates
Country: GB
Zip Code: M1
Location: Manchester, England
HWID: C14ED47E2CD51DFE09E61A632521
Current Language: Somali
ScreenSize: {Width=946, Height=873}
TimeZone: (UTC+08:00) Perth
Operation System: Windows Vista x32
UAC: AllowAll
Process Elevation: False
Log date: 5/28/2023 4:42:33 AM

Available KeyboardLayouts:
Chinese (Simplified)


Hardwares:
Name: Intel(R) Core(TM) i5-1537 CPU @ 2.67GHz, 9 Cores
Name: VMware SVGA 3D, 4293918720 bytes
Name: Total of RAM, 14199.50 MB or 14539776 bytes


Anti-Viruses:
Bitdefender
```

Here we see a Country/Location that does not match the TimeZone or the Keyboard layout

```
**********************************************
*                                            *
*   ____  _____ ____  _     ___ _   _ _____  *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____| *
*  | |_) |  _| | | | | |    | ||  \| |  _|   *
*  |  _ <| |___| |_| | |___ | || |\  | |___  *
*  |_| \_|_____|____/|_____|___|_| \_|_____| *
*                                            *
*  Telegram: https://t.me/redline_market_bot *
**********************************************

Build ID: lina
IP: 146.70.99.219
FileLocation: C:\Users\Easdf\Office\Ra5eMzTjx.exe
UserName: LDugmore
Country: DE
Zip Code: 65931
Location: Frankfurt am Main, Hessen
HWID: 5B9762CE1CF21FBF93ACE67
Current Language: Spanish (Puerto Rico)
ScreenSize: {Width=789, Height=1717}
TimeZone: (UTC-04:00) Caracas
Operation System: Windows 8 x32
UAC: AllowAll
Process Elevation: False
Log date: 5/28/2023 3:32:56 AM

Available KeyboardLayouts:
Arabic (Eritrea)


Hardwares:
Name: Intel(R) Core(TM) i5-8089 CPU @ 1.57GHz, 9 Cores
Name: VMware SVGA 3D, 4293918720 bytes
Name: Total of RAM, 10696.15 MB or 10952704 bytes


Anti-Viruses:
Avira
```

Same issue here – information does not make sense

```
URL: https://discord.com
Username: HGeery@fanniemae.com
Password: gKmT3qQPAsPH
Application: Cyberfox_Default
===============
URL: https://www.roblox.com
Username: EWisor@morganstanley.com
Password: iWiZo9Rti18
Application: Cyberfox_Default
===============
URL: https://steamcommunity.com
Username: IrrEstella@calpine.com
Password: eB9oUDOa9k10b
Application: Cyberfox_Default
===============
URL: https://www.amazon.com
Username: Kassey.Mcgiveron@microsoft.com
Password: 5ExI1LUk
Application: Cyberfox_Default
===============
URL: https://login.live.com
Username: Evelyn.Didomizio@unitedhealthgroup.com
Password: 8De1eb8F
Application: Cyberfox_Default
===============
URL: https://eu.battle.net
Username: Judith.Chaffins@grainger.com
Password: HbRAOst6
Application: Cyberfox_Default
===============
URL: https://netflix.com
Username: MeldrumRea@express-scripts.com
Password: yUurZIEg3
Application: Cyberfox_Default
===============
```

Way too many unique emails in here

Nothing in common about them, either

Red Team Infostealer Protocol

A system for leveraging infostealer data

What is the goal of this protocol?

To “keep calm and analyze on”

- Each infostealer log has thousands of data points
- It is easy to get distracted and miss things
- We need a plan to stay organized

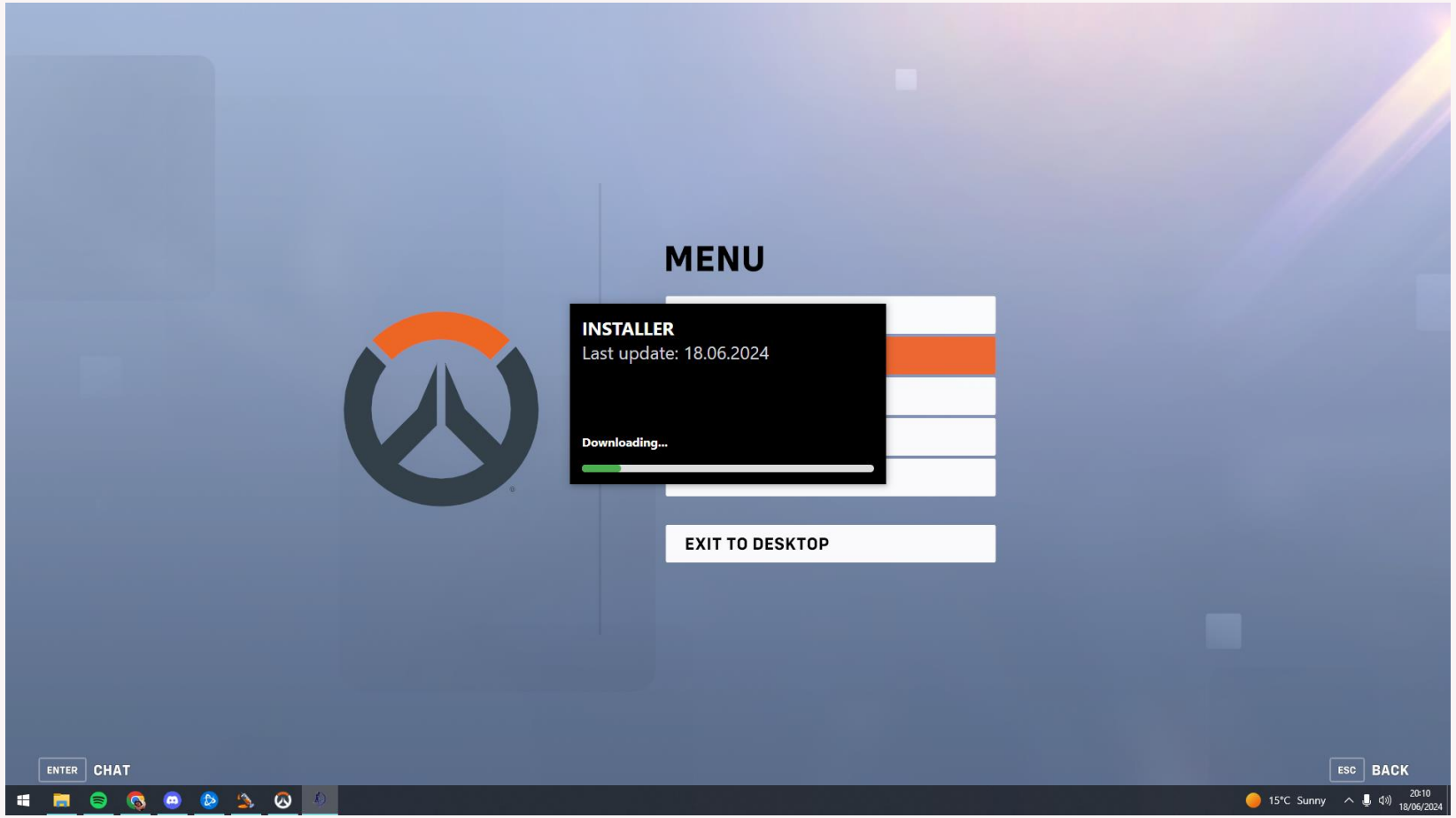
Choose one of the synthetic logs from the Github site and try to answer the following.

Section 0: Information about the infection

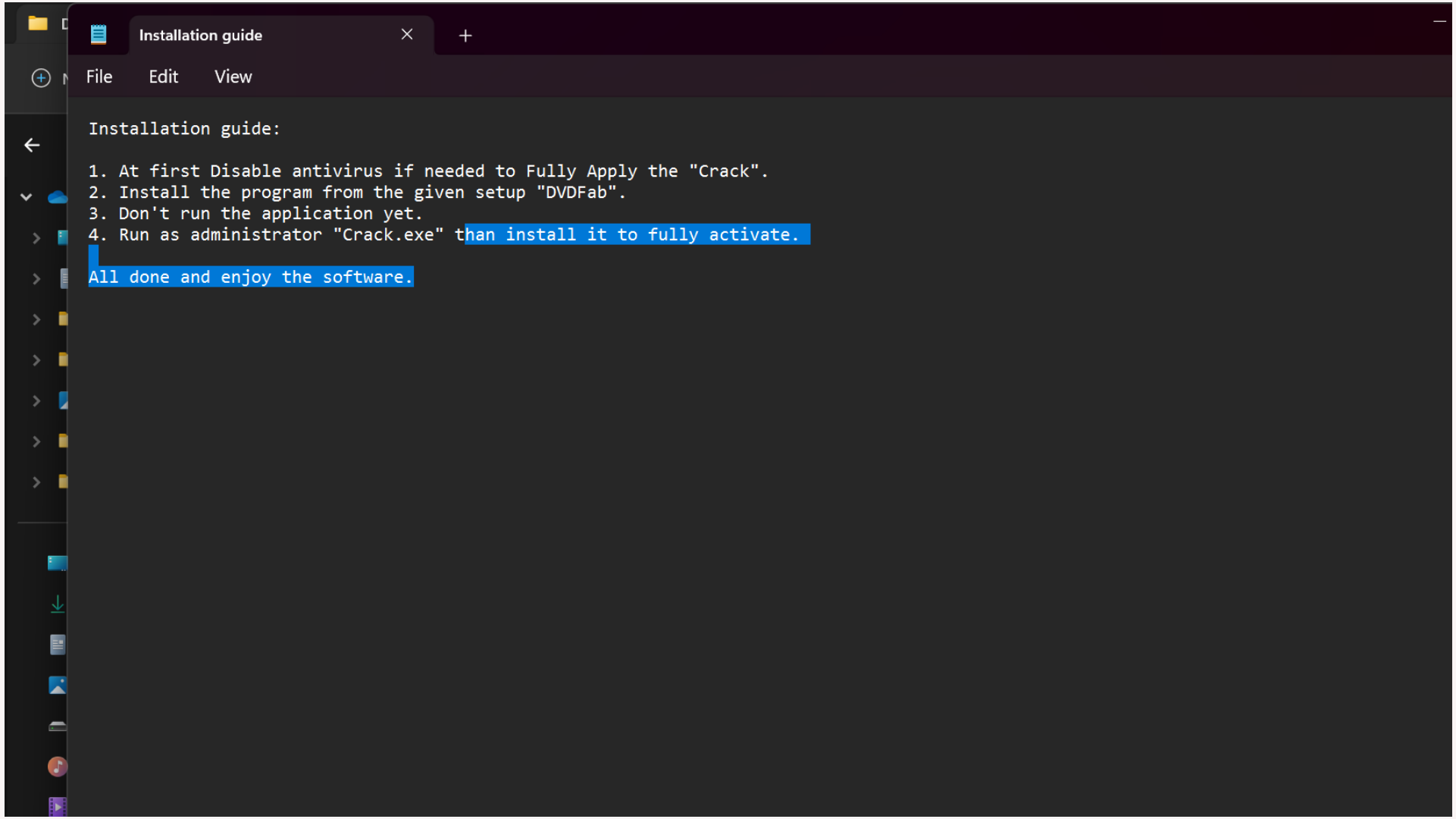
Here we summarize the high level info about this infostealer infection

- [ ] Infostealer infection date (see header file - be careful of month/year confusion):
- [ ] Infostealer family (see header, YARA rules):
- [ ] Likely infection vector (see screenshot, history):
- [ ] Other notes about infection:

Here is a real sample “moment of infection” screenshot (since the synthetic ones are fake)



Here is another sample



Section 1: Basic information about the target

Here we summarize the high level info about this target; Most of this info will come from the autofills

- [ ] Full name(s) and name variant(s):
- [ ] All primary and alternate email addresses:
- [ ] Phone number(s):
- [ ] Username(s):
- [ ] IP Address (from header file):

Section 2: Inventory of target's browser profiles

Studying the profiles will help us understand complexity of account behavior

How does the target use browser profiles?

- ☐ Single profile
- ☐ Multiple profiles
  - ☐ Profiles represent multiple IRL identities (e.g. parent/child)
  - ☐ Profiles represent multiple online identities (e.g. work/home, personal/gaming, secure/insecure)
  - ☐ Multiple profiles for other/unknown reason
- ☐ Notes:

Multiple browser profile summary

Line	Profile Name	Folder	Notes
Example	*Chrome Default*	*/Chrome/Default*	*main computer owner's profile*
1			
2			
3			

Optional: handy, dandy table for keeping track

Section 3: Inventory of target's interests

Here we log the target's personal interests and counts

Example:

- [x] Gaming: Twitch (3 logins), Roblox (5 logins), Steam (multiple)

Inventory:

- [ ] Dating sites:
- [ ] Gaming:
- [ ] Gambling:
- [ ] Health/medical:
- [ ] Financial services:
- [ ] Parenting/family:
- [ ] Social media accounts:
- [ ] Messaging apps:
- [ ] Cloud Storage:
- [ ] IT/Programming/SysAdmin:
- [ ] Other:

Section 4: Assessment of target's password behaviors

What does the target's password behavior tell us about their security habits?

Password Behaviors

- ☐ Reuses same password for multiple logins
  - ☐ Password reuse follows username or email
  - ☐ Password reuse follows site type (business logins get one type of password, gaming logins get another password)
- ☐ Uses variations of base password
- ☐ Keyboard patterns (qwerty, 123456)
- ☐ Personal info in passwords (names, dates)
- ☐ Appears to use password manager
- ☐ Notes:

Section 5: Target's Corporate Access

Which types of relevant corporate accounts does this target have, according to the infostealer logs?

Table summarizing target's corporate access as shown in logs, if any

Line	System/URL	Username	Password	Notes
Example	*portal.company.com*	*johnSmith*	*password123*	*reused on personal sites*
1				
2				
3				

Summary of corporate account types

- ☐ Developer (GitHub, GitLab, IDE logins):
- ☐ IT/Admin (AWS, Azure, admin panels)
- ☐ Finance (QuickBooks, banking portals)
- ☐ HR (Workday, BambooHR, payroll)
- ☐ Sales (Salesforce, HubSpot, CRM)
- ☐ Executive (board portals, investor sites)
- ☐ Notes:

Wrapping Up

Where to go next

Resources

Here are some handy places to get more info

- Megan’s Synthetic Infostealers Github
- What is this stealer? Github

QUESTIONS?