



Tracing the Intrusion: Unveiling the Covert Trails of Infostealer Malware Ecosystems

Pavan Karthick M
Threat Researcher, CloudSEK



Agenda

- Introduction
- What damage can infostealers do
- Case study – Major Cyber attack
- Trafflers & their Ecosystem
- Delivery Mechanisms & Evolution
- Trends
- Motivation
- Mitigation & Concluding Notes



5 Most Dangerous Cyber Attacks

according to SANS

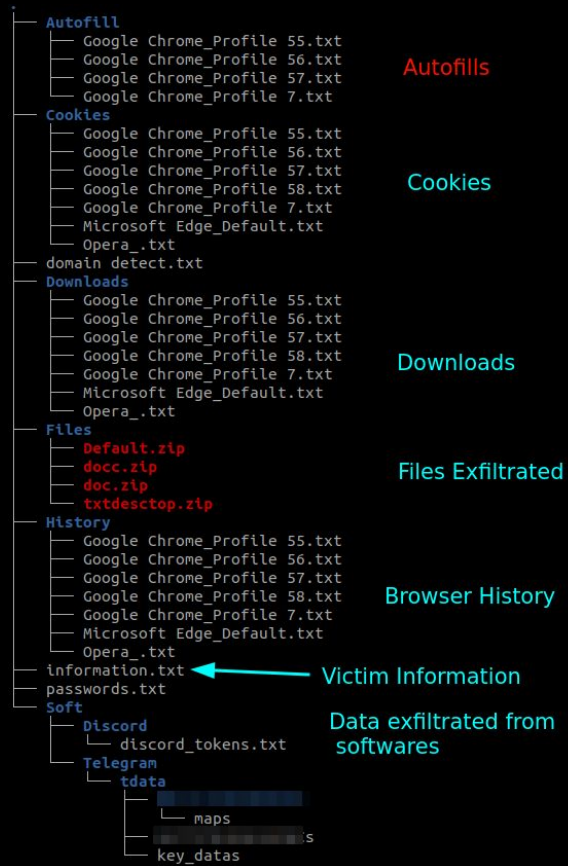
- SEO Boosted attacks
- Malvertising
- Developers as target
- Offensive uses of AI
- Weaponizing AI for Social Engineering

Introduction

- Infostealer – What is it ?
- What enables it ?
- Infostealer capabilities
 - Packers – Hides payload
 - Loaders – Drops payload
 - Defender, AMSI and EDR Bypasses
 - Exploiting CVEs - They are on track with latest security trends!
 - Updated with exfiltrating data of most used software.

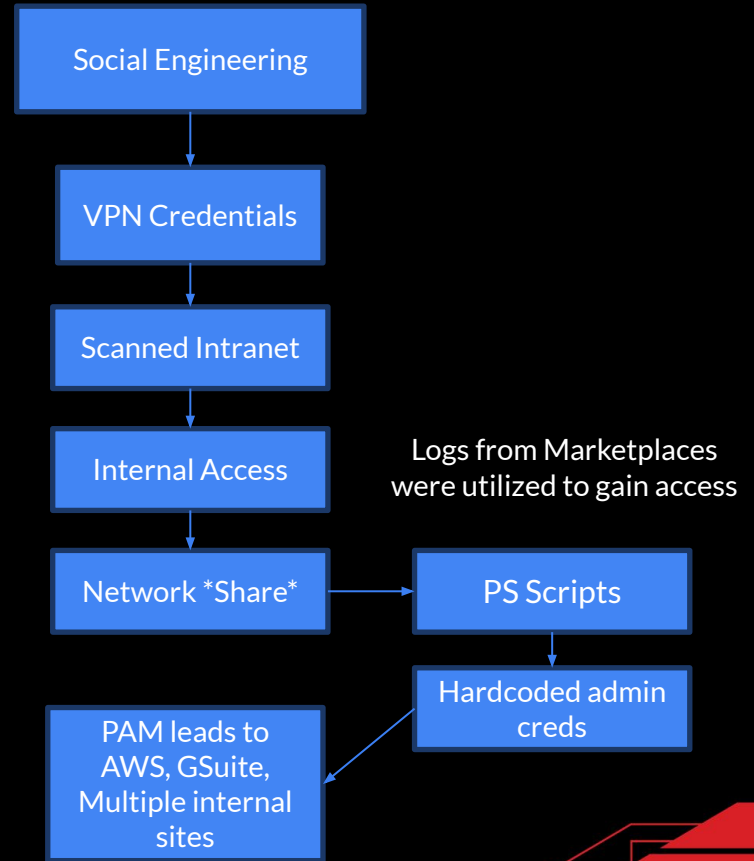
What happens if you are infected

- Data gets compromised across synced devices.
- Exploited multiple times by multiple threat actors.
- Victim's browser is mimicked and IP impersonation to bypass 2FA, IP based login

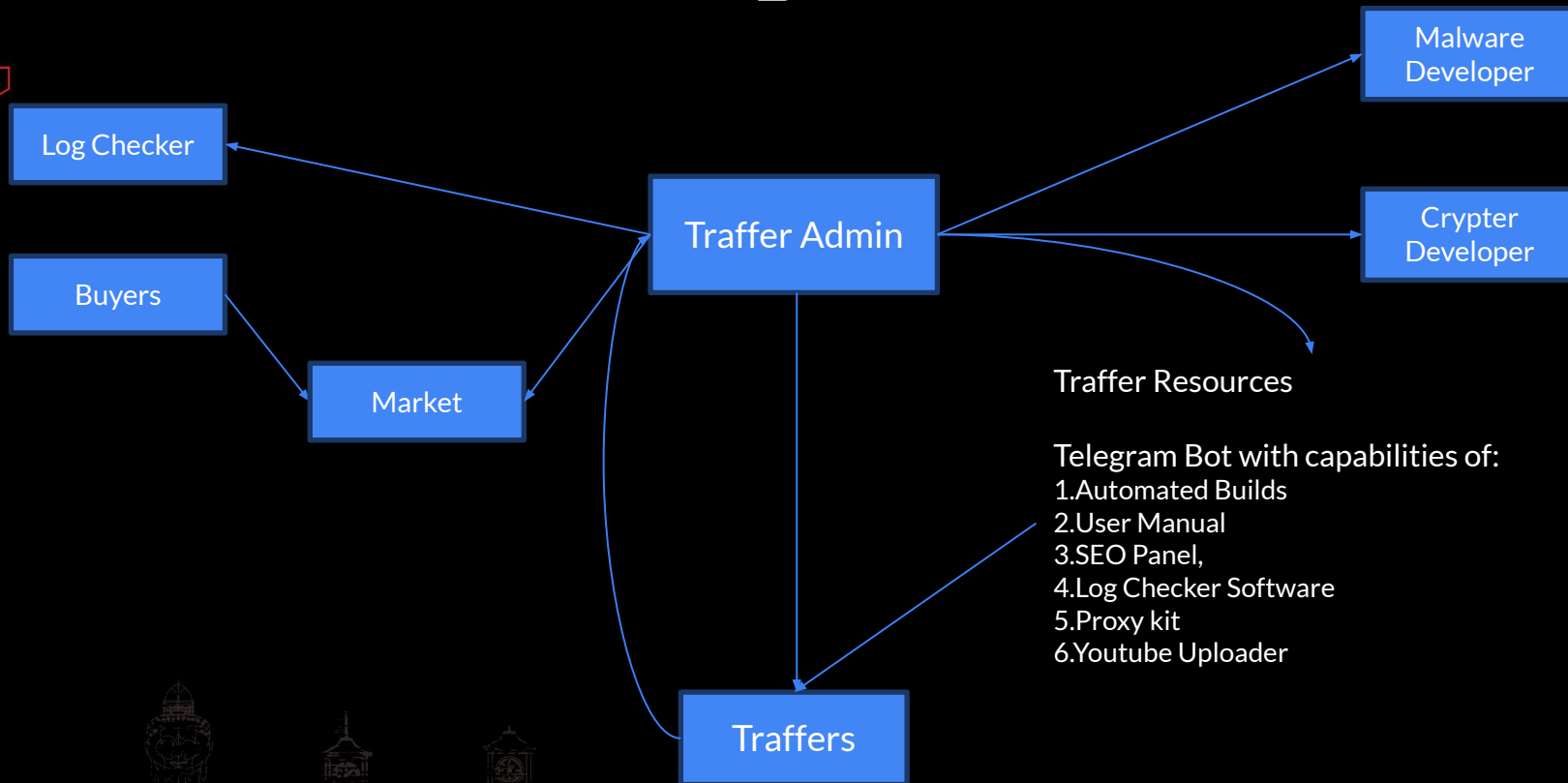


Case Study

- Cyber attack was on a organization with ~\$30B Revenue
- Minimal Skill
- Maximum Damage
- Used by every TA



Traffer Ecosystem



Delivery 1 - Malicious Domains

Your Download Link is Ready
Copy below download link and paste into new tab.
Copy Link ↓

File Password is: 10101

Download Link Copied, Open in New Tab

Annotations:
 - Cheap Domains (Behind Cloudflare) points to the URL bar.
 - Redirector 1 and Redirector 2 point to the main content area.
 - Redirector 1x and Redirector 2x point to the network tab.
 - Shortners points to the main content area.
 - Malware Archive points to the main content area.

Status	Method	Domain	File Name	Type	Transferred	Size
200	GET	mat4bl3eb.cfd	/https://s4ozpyrr8.cfd/?j=155&r=Microsoft-Office-2010-crack---100-Working-product-key=2023-&adcode=	document	983 B	166
200	GET	mat4bl3eb.cfd	/https://mat4bl3eb.cfd/?LHjaiQv3Td=OKN6qESbRf1voileyBJla7wpTGkXdHMU0453YLcz=1	document	599 B	225
200	GET	mat4bl3eb.cfd	/1LHjaiQv3Td=OKN6qESbRf1voileyBJla7wpTGkXdHMU0453YLcz=1KA13ToysOSrjVx/	document	1.46 kB	15
200	GET	mat4bl3eb.cfd	all.css	stylesheet	13.17 kB	147
200	GET	mat4bl3eb.cfd	style.css	stylesheet	1.67 kB	247
200	GET	mat4bl3eb.cfd	jquery.js	script	32.46 kB	177
200	GET	mat4bl3eb.cfd	common.js	script	1.30 kB	17
200	GET	fonts.googleapis.com	css2?family=Montserrat:wght@100;200;300;400;500;600;700&display=swap	stylesheet	1.30 kB	17
200	GET	mat4bl3eb.cfd	sQEFD.png	img	602.40 kB	84
200	GET	fonts.gstatic.com	JTUSjlg1_i6t8kCHKm459Wlhwy.woff2	font	31.76 kB	26
200	GET	mat4bl3eb.cfd	fa-solid-900.woff2	font	76.82 kB	82
200	GET	fonts.gstatic.com	JTUSjla1_i6t8kCHKm459Wlhwy.woff2	font	31.76 kB (raced)	11

SEO Enhanced
Amazing Templates
Crawling Detection
Anti-Analysis
Mimicking legit sites

Personalize your experience

You can use our catalog on the site and download the software you like. Or try our application with 100+ free and full programs!

[Download for Windows](#)


Personalize your gaming experience

Thousands of free mods and trainers for your favorite single-player PC games — all in one place.

Visit us on your PC to download the app
[Download anyway](#)

4.9/5 Trustpilot rating

▶ How WeMod works



We use cookies to understand how you use our site and to improve your experience. This includes personalizing content and advertising. By continuing to use WeMod, you accept our use of cookies, revised [Privacy Policy](#) and [Terms of Use](#).

[Got it](#)

Delivery 2 - 911 Infection chain



YouTube

Targeted Infostealer attacks

Sourcing Compromised YTL

Mail Spam

Cheap Proxy Service

Anti-D

Trading Platform - IM and SOCIAL NETWORKS: accounts, gr...

YOUTUBE FROM 1k SUB 5-11 REGI NEED HUNDREDS OF THOUSANDS OF LOGS

KingYoutube · Dec 2, 2022

ESCROW AVAILABLE IN THIS THREAD!

New deal

File Edit View Window Help

Name Status

Любов

II STOP NO STATUS

(12) YouTube

www.youtube.com wants to

Show notifications

Allow Block

Musique Joueur du Grenier Jeux Supercar Conduite de ve...

Actual

permanen... vide... les 1 top plus les... avec une... les

Junidaine: dite qu'avant tu faisais 100k viewers...

Junidaine: pk t'as quasiment plus de viewers ? sardoche a banne j... **STU GLOWSON**

Sardoche ne fait plus 100k viewers...

Sard Clip 3.0 k vues · il y a 2 heures

Abonnements

Bibliothèque

0:42 1:00:52 03 1:56:03

MAHDI BA TV

BRASQUEURS À 16 ANS (une très mauvaise idée)

PENSIONNAT DE CHAMPAGNE #3 - EMBROUILLÉ AU PIANO

MahdiBaTV 646 k vues · il y a 5 mois

JirayaTV 376 k vues · il y a 1 an

C'EST MOI LE CHEF

11:07 3:04 7:19

NENVOYEZ SURTOUT PAS VOS ENFANTS ICI ! (je suis choqué)

PandamanTV 36 k vues · il y a 2 semaines

Best reactions in a Toyota Supra compilation

ARAVIS 7,6 M de vues · il y a 5 ans

Au Nom du Jour où Tout a Basculé - Le Monde à l'Envers

Le Monde à l'Envers 9,4 M de vues · il y a 7 ans

CARROSSIERE RESTAURATION ?

TAXI 5 AMBOS VS BUCCO

ZAP DE TWITCH

Memory: 0 GB

Screen: Real

Audio: Real

Media devices: Real

Do not track: Off

Paste your cookies or drag and drop your file here

COOKIES FROM FILE

Delivery 2 - Contd..



Infostealer Execution

Posts Posted

Data Exfiltration



YouTube

Archive with Massive compression ratio

C:\Users\mpkar\Downloads\App-Zone_pas2023.rar\

File Edit View Favorites Tools Help

Add Extract Test Copy Move Delete Info

C:\Users\mpkar\Downloads\App-Zone_pas2023.rar\

Name	Size	Packed Size	Modified
PROPAMAT	130 316 387	55 174 528	2023-08-21...
Templates	592 916	191 680	2023-08-13...
CrystalDecisions.S...	872 448	237 264	2023-01-25...
Installplus_1.038.6...	819 724 776	7 731 392	2023-08-21...



C2

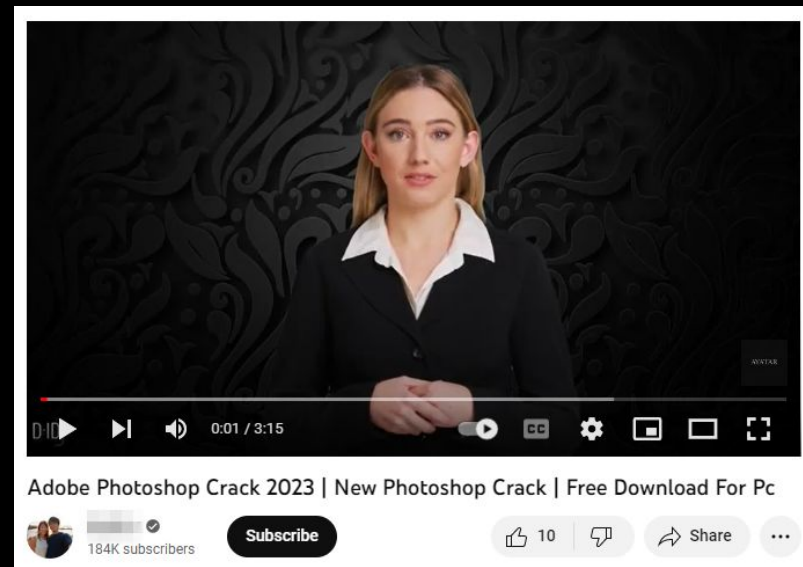
1,872 views Premiered 7 hours ago #Filmora12 #Filmora12Free #patilalyadv

Delivery 3 – Mail Spam

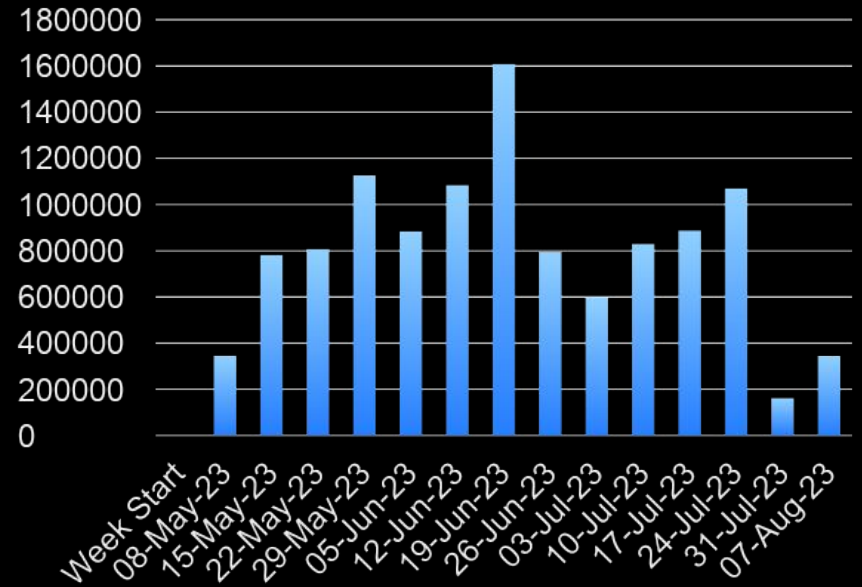
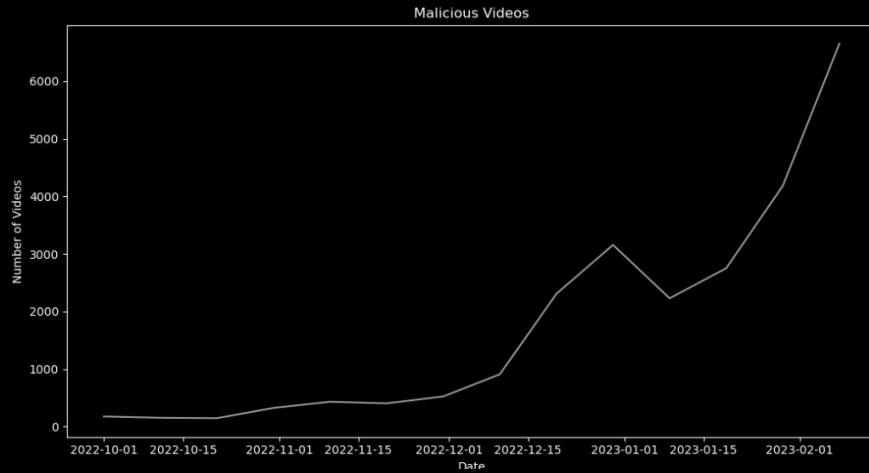


Infection Chains keep Evolving with one Single goal ☐ To Steal Data

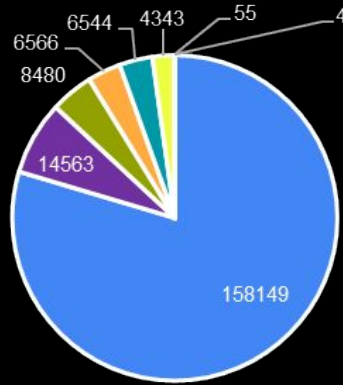
- Usage of AI Generated Voice overs and Personas to feature in their videos
- Constantly evolving & diverse tactics
- Achieving business continuity by usage of compromised accounts
 - To run their infrastructure of hosting malware
 - Deceive users into believing the content is genuine



Trends

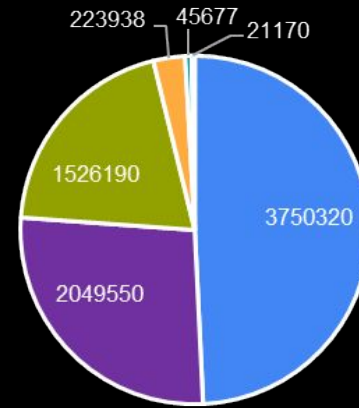


Infostealers Detected (May-Aug 23)



- Not Detected
- Vidar
- RedLine
- LummaStealer
- Raccoon Infostealer
- Recordbreaker
- Stealc
- Other

Infostealer Families Prevalent in market

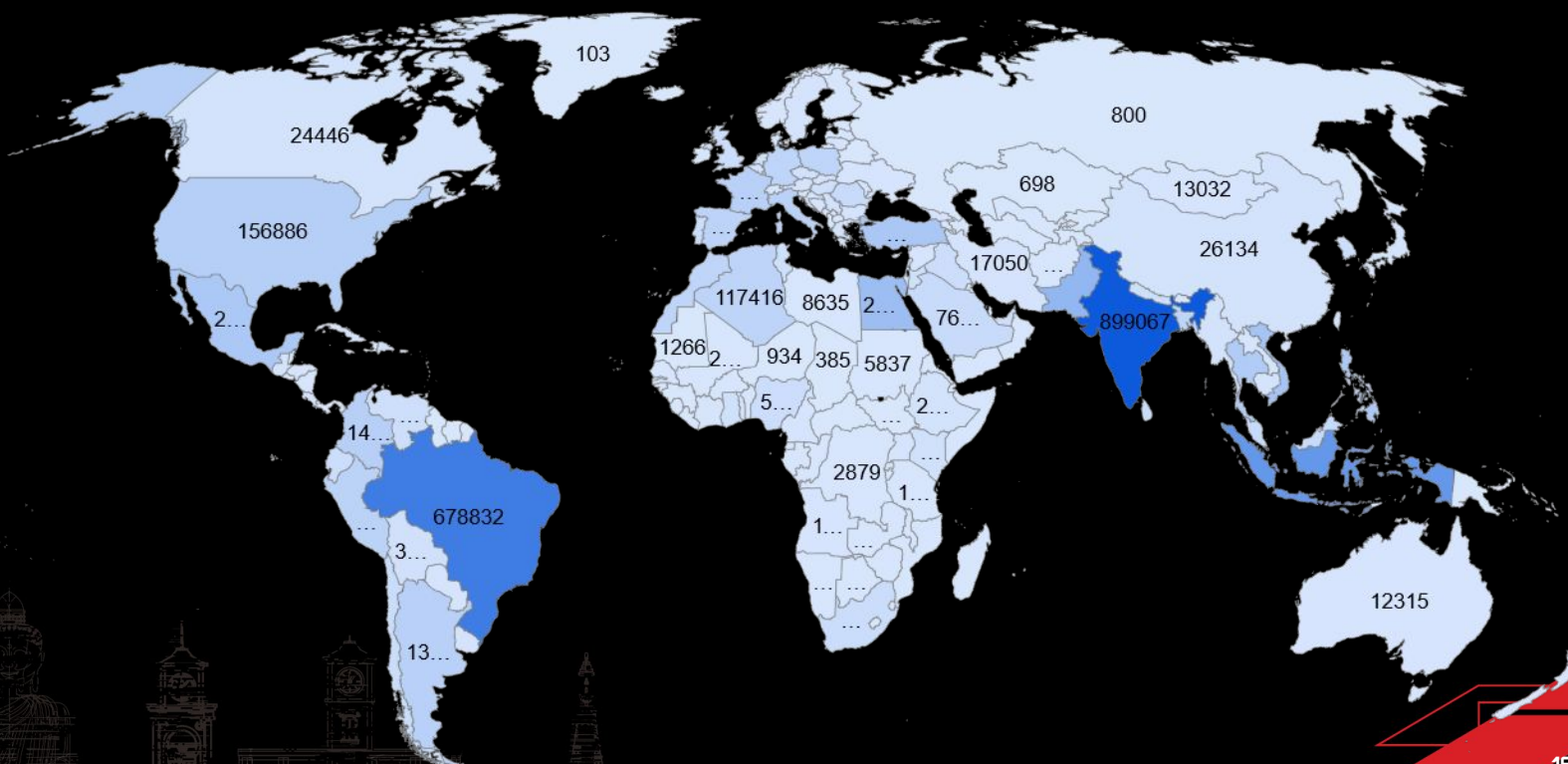


- racoon
- vidar
- redline
- lumma
- silencer
- risepro

Data Logs on Sale in Darkweb Marketplaces




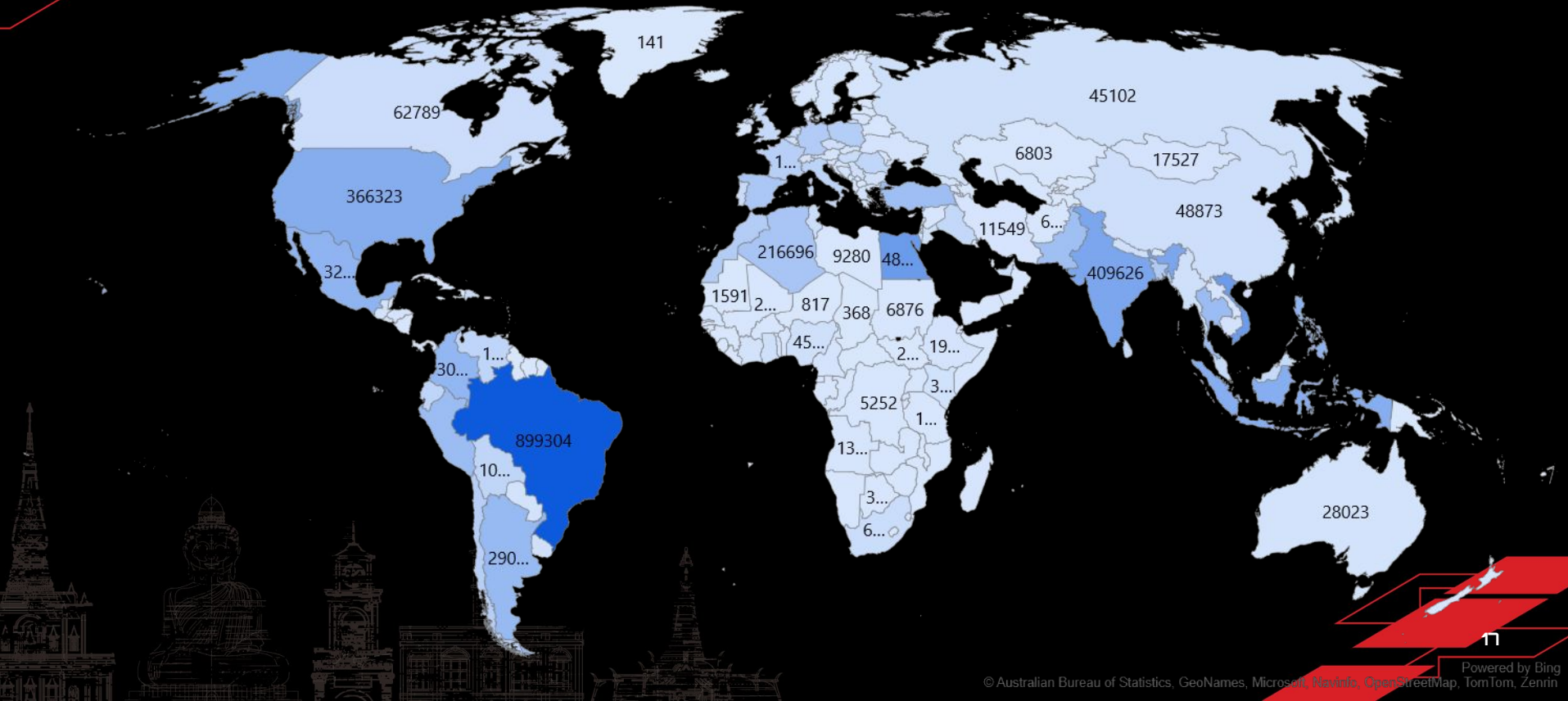
Logs on sale*



Infection Logs From multiple sources



count 
110 899304



Motivation ?

- Lot of scope to earn for a skilled TA
- Zero to Hero training by TA for TA
- Less knowledge of the public around malicious software
- Money 💰
 - Potential > \$100k USD

English

🏆 Best traffers of all time (logs):

1. @moriwWs | Logs: 5454
2. @LEORIC1337 | Logs: 3019
3. @WhyMelol123 | Logs: 2757
4. @FlexFun228 | Logs: 2686
5. @reimann_money | Logs: 2275
6. @nickosUWU | Logs: 2260
7. @ZEDSS0 | Logs: 2016
8. @laveelii | Logs: 1858
9. @ozabo4en | Logs: 1756
10. @zhilsholi | Logs: 1756
11. @Averdar | Logs: 1654
12. @o1p3n | Logs: 1647
13. @krxstkrxst | Logs: 1573
14. @zoro_one | Logs: 1463
15. @pak_1111 | Logs: 1442

What Do We Do ?

- Continuous Evolution & Automation in proliferation requires same proactive Automated Detection and Mitigations
- IoCs & YARA rules seem useless due to the sheer volume of infection chains possible in terms of Domains, samples, C2s.
 - Enforcing MFA & Strict session limits (For internal websites)
 - Organizations following BYOD policy should add windows policies locally which can prevent storage of passwords on browser.
 - Regular awareness training.
 - Paid software should be made available.

THANK
YOU!

