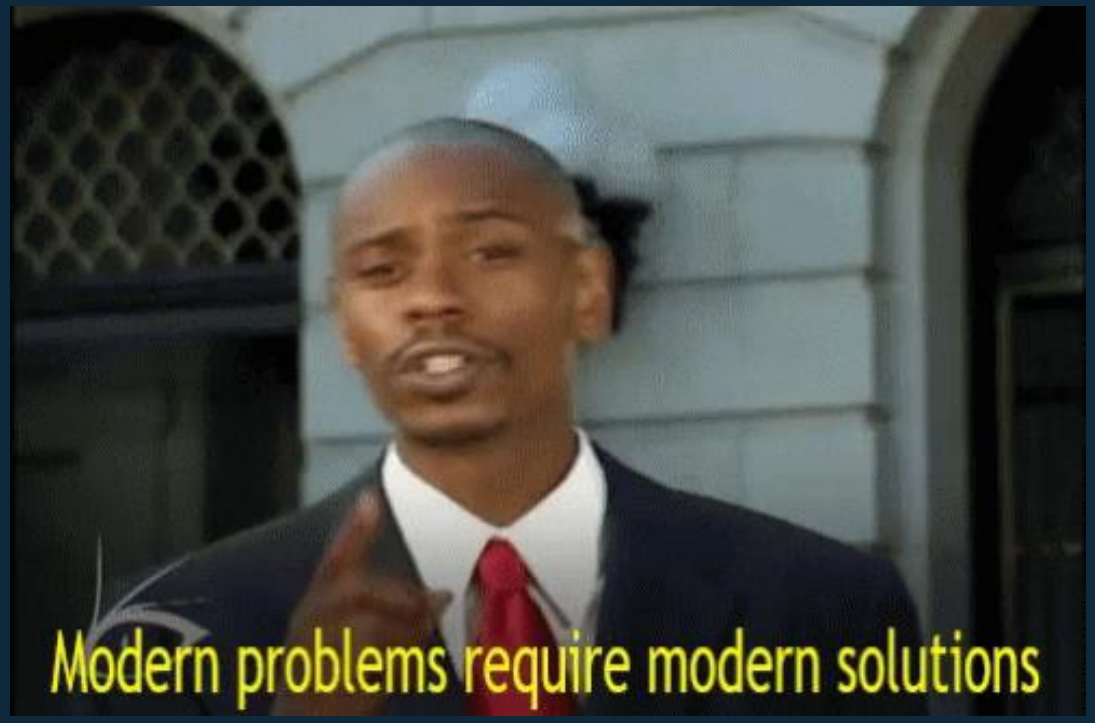
Cyber Threat Intelligence: Where Should You Start?

National Cyber Security Congress

Presented by: Alyssa Berriche

Introduction

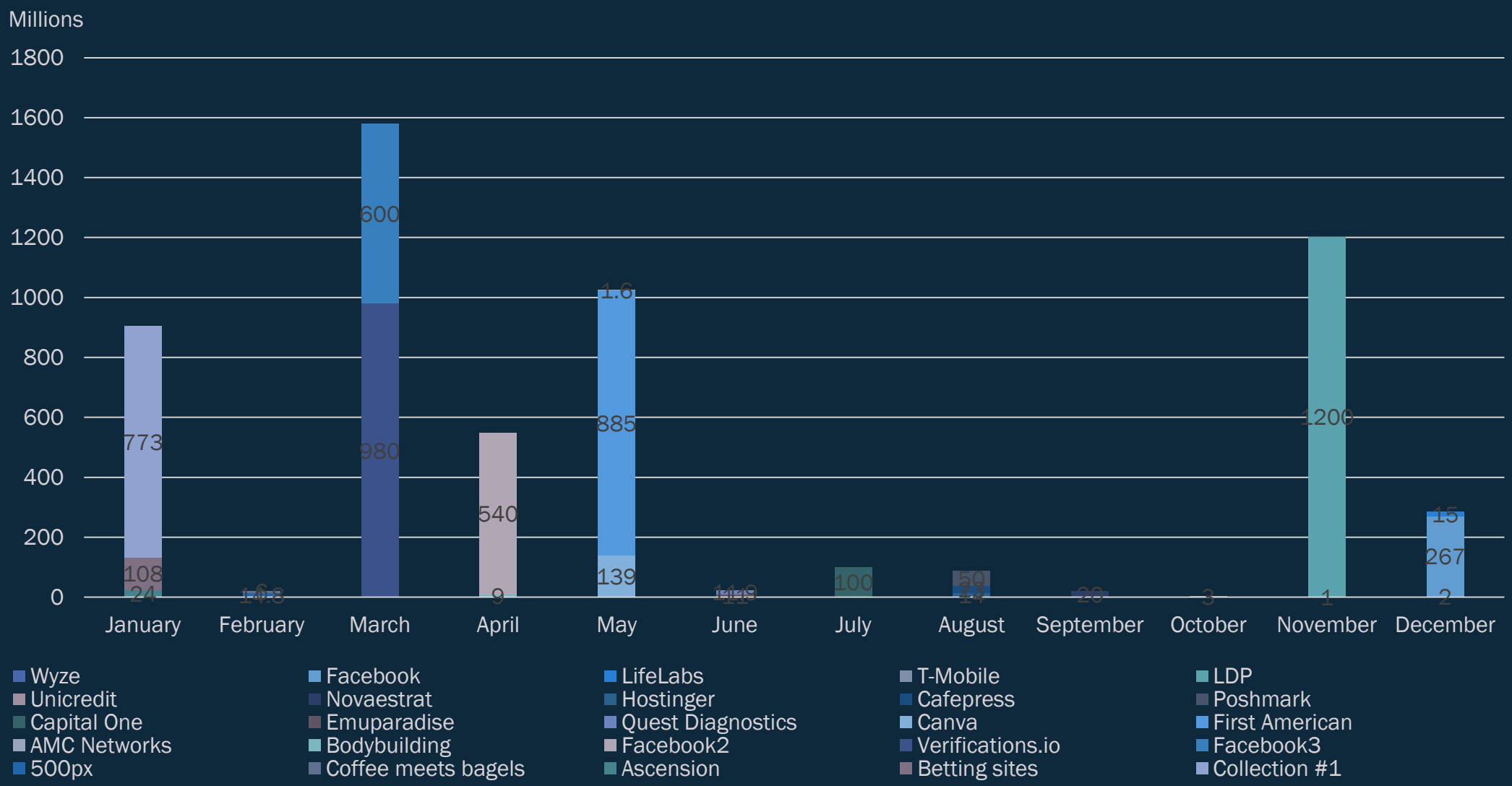



Breaches
Phishing
Credential stuffing attacks
APTs
Exploits
Landscape
Supply chain attacks
DDoS
Crypto-mining
Fraud activities
Social Engineering
Malware infections


ME SUBSCRIBING TO ANY NEWSLETTER AND SUSPICIOUS WEBSITE
USING MY OFFICIAL EMAIL ADDRESS
imgflip.com


HOW DID PHISHERS GET
MY EMAIL ADDRESS?
imgflip.com

Most impacting breaches of 2019



Modern problems

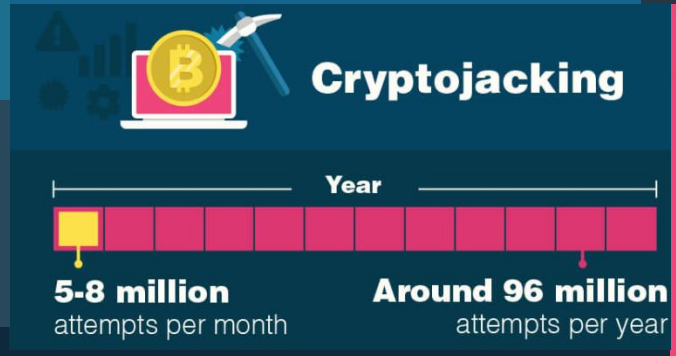
This year organizations and individuals will pay approximately $11.5 billion because of ransomware.

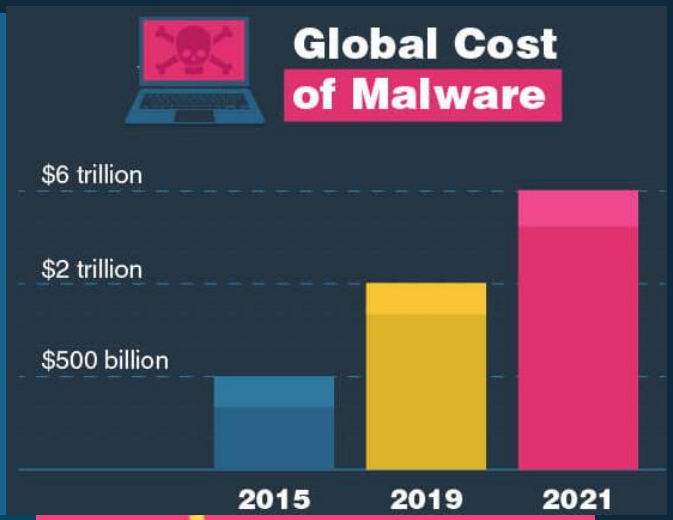
24,000 malicious apps are blocked every day.

76% of businesses reported being a victim of a phishing attack in the last year.

(Wombat Security, 2019)

As much as 38% of malware is now being disguised as a Word doc.





Your home network or business still isn't prepared for a cyberattack.

- The purpose of **threat intelligence** is to provide a deep and accurate analysis of the cyberthreats, to help companies counter them.

WHY?

“

Keep your friends close but your enemies closer.

The Godfather Part II

Who needs Threat Intelligence

Because “Security is everyone’s concern and responsibility”

Benefits of Threat Intelligence

- Useful for companies struggling with skills shortage
  - Because it helps reducing number of alerts, false positives
- Provides context about emerging threats
  - Resilience
  - Improve ability to defend against cyberattacks
- Helps decision makers to prioritize response, or investments in technology and people
- Faster response to threats

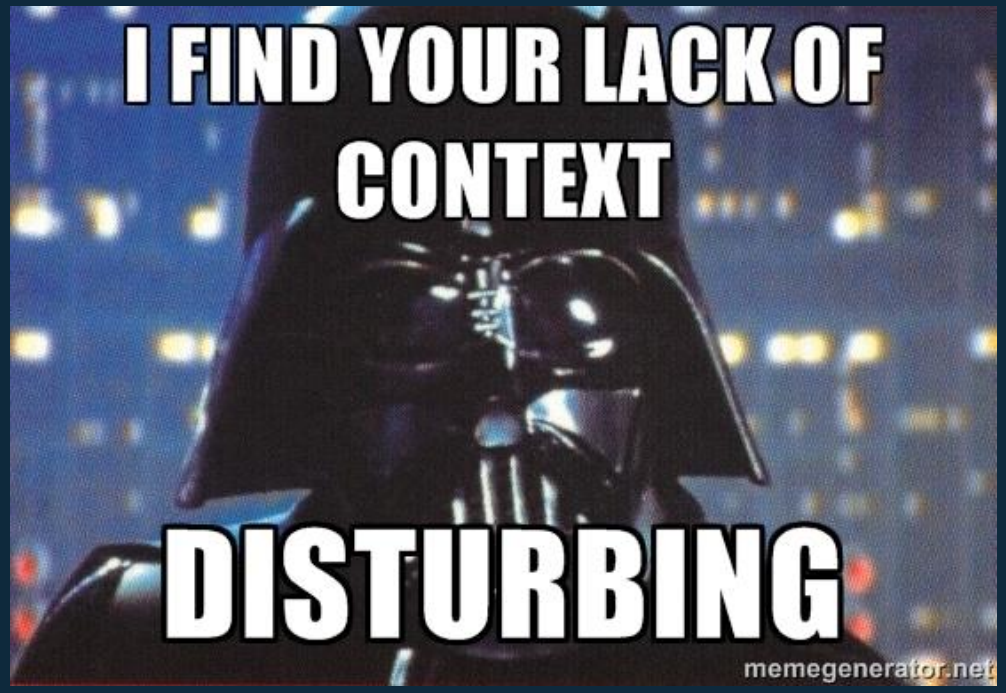
Threat Intelligence for Incident Response

- Reducing false positives
- Enriching alerts with real-time context, like custom risk scores
- Comparing information from internal and external sources

➔ Faster identification of threats

Use case 1: reactive hunting

- Based on alerts and detections
- Extract indicators and enrich them with context
- Create your TTPs
- Understand your adversaries
- Hunt for additional IOCs



Use case 2: uncovering hidden attacks

- Search for relevant emerging threats shared by different sources (ISACs, CERTs, vendors, resarchers, …) in your environment

Threat Intelligence for Vulnerability Management

Patch everything, All the time

Patch prioritizing based on risk

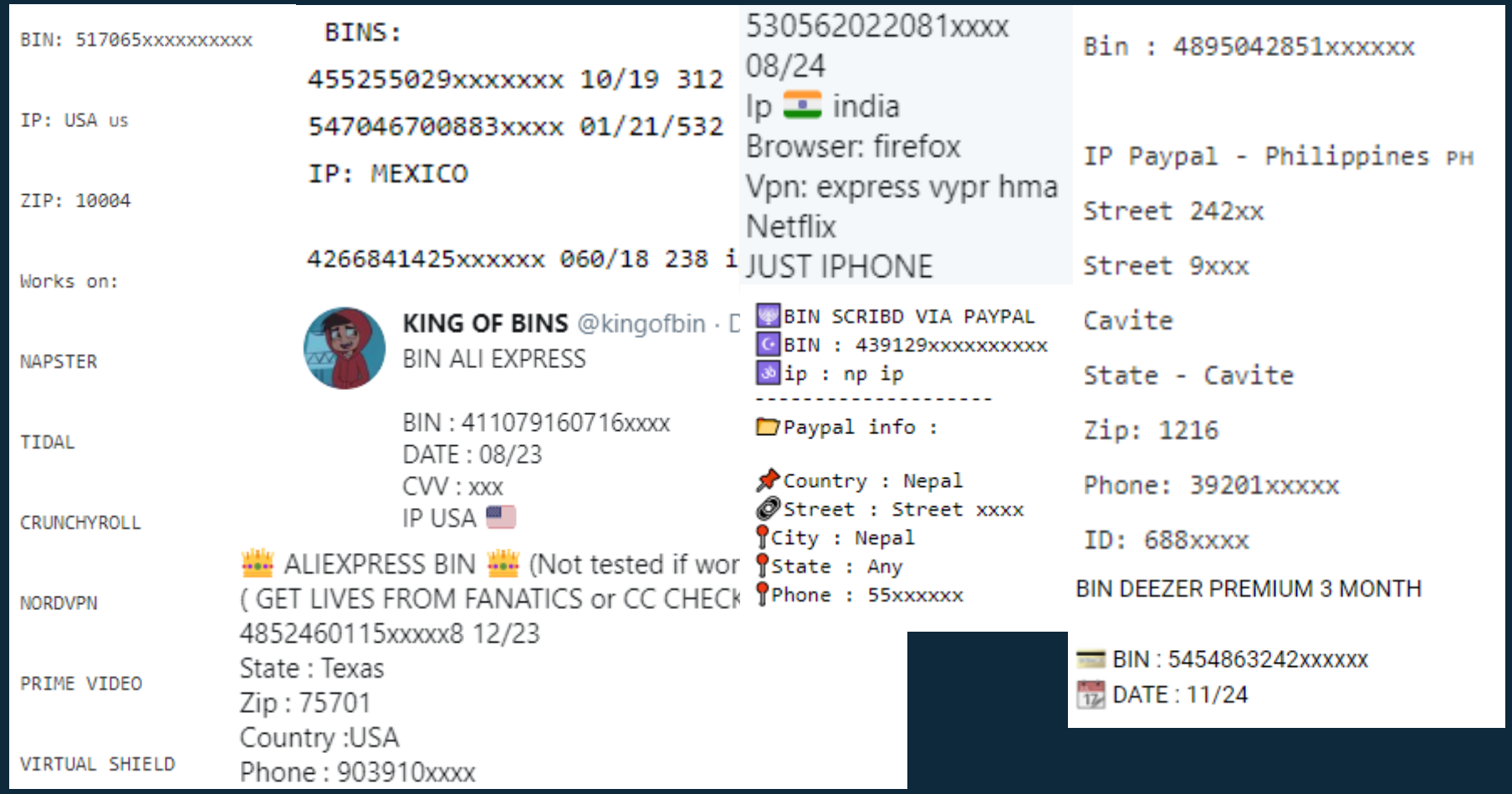
Use case: WannaCry

- WannaCry propagated through EternalBlue exploit, developed by US National Security Agency (NSA) and exposed/ released by Shadow Brokers after the MS17-010 patch

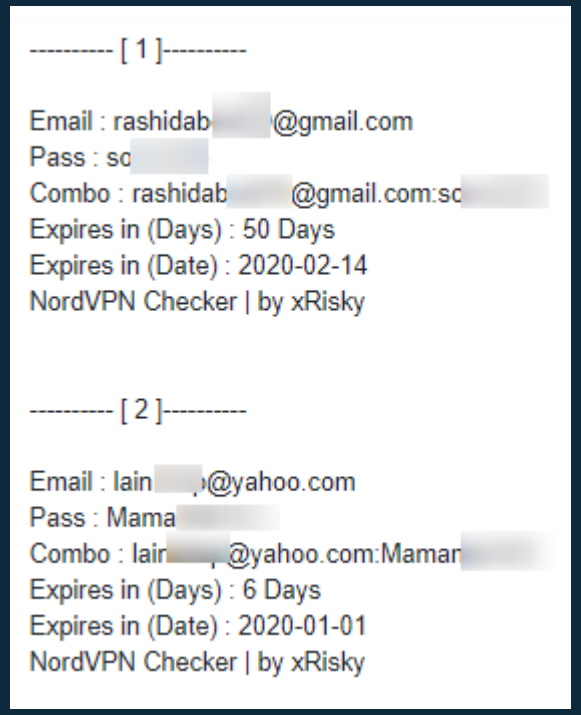
Threat Intelligence for Fraud Prevention

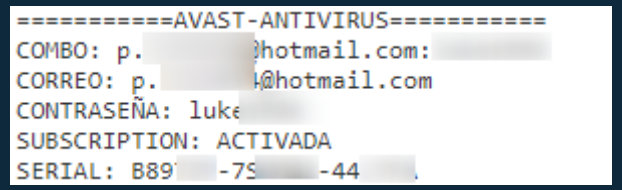
- Monitoring sources like criminal communities, paste websites and forums for relevant banking information
- Monitoring for compromised data from forums, underground marketplaces, pastes, leaked combos lists,…
- Monitoring for domains and website mimicking official ones to steal credentials, sell counterfeit, promote fake deals, …

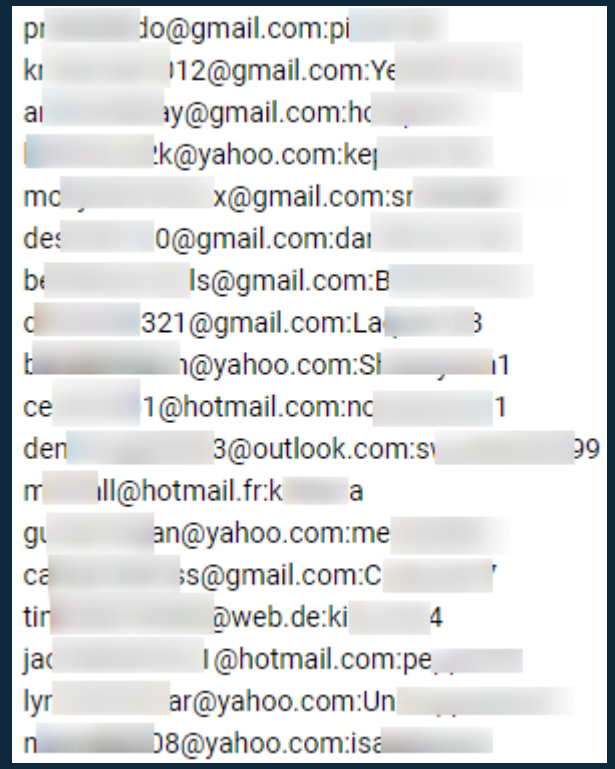
Use case 1: Banking information

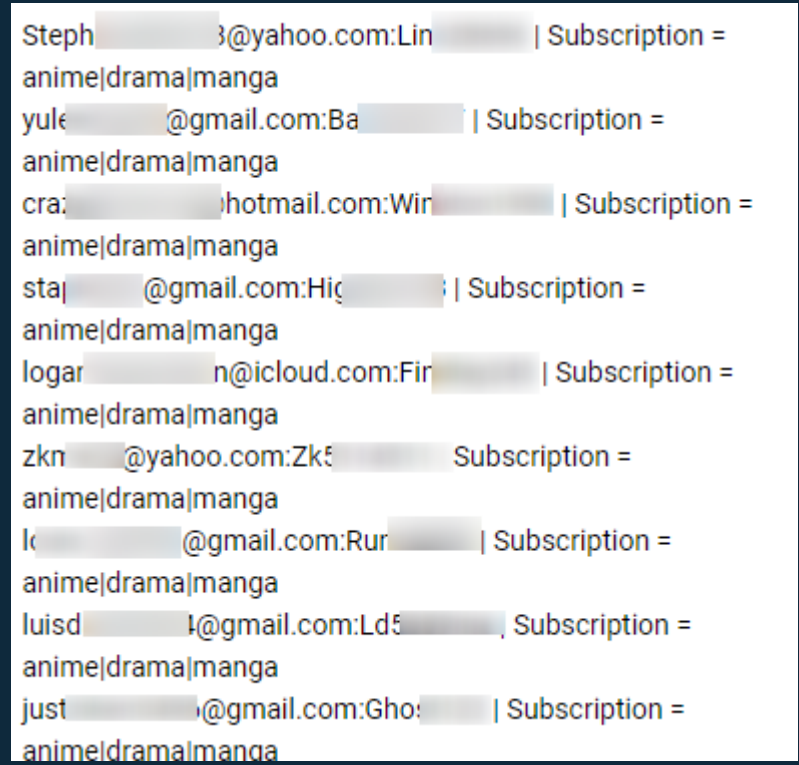


Use case 2: Compromised data

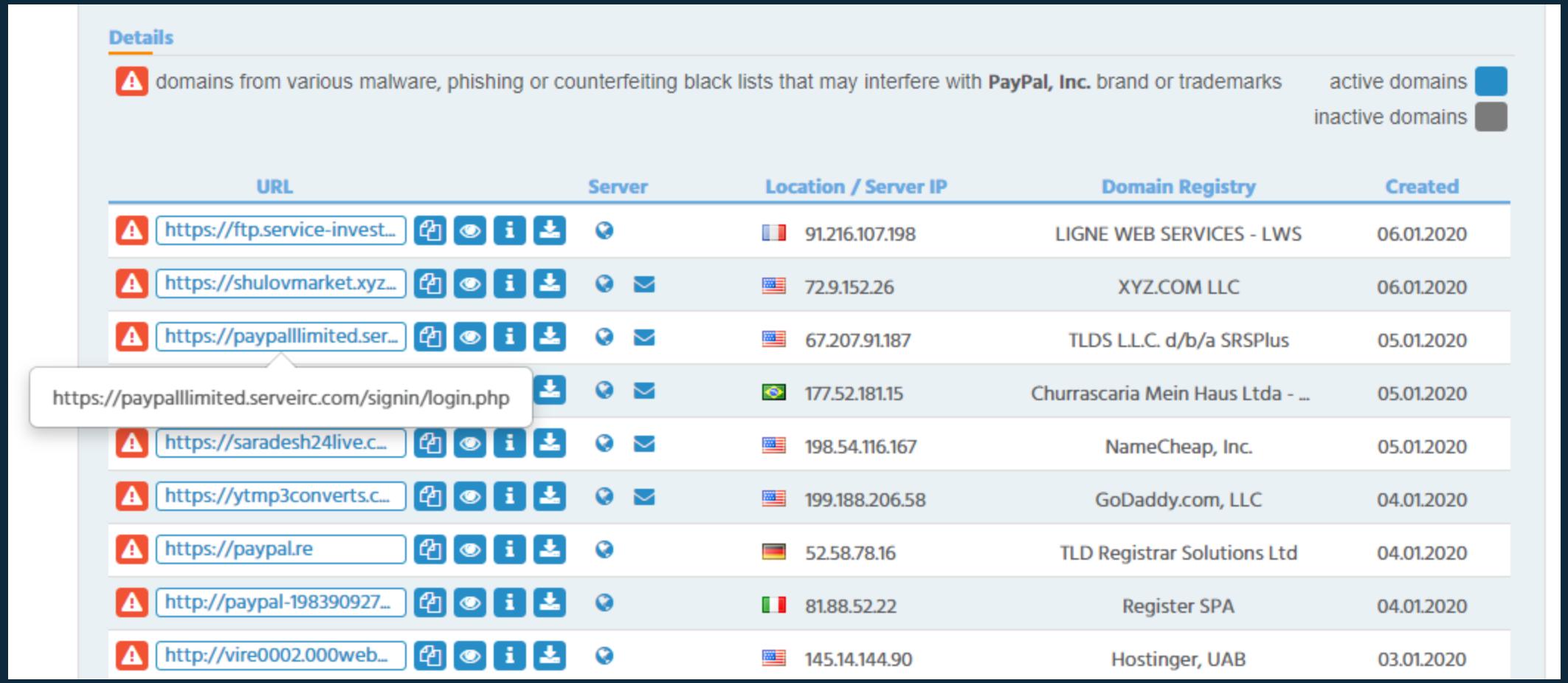








Use case 3: typosquatting



Details

domains from various malware, phishing or counterfeiting black lists that may interfere with **PayPal, Inc.** brand or trademarks

active domains

inactive domains

URL	Server	Location / Server IP	Domain Registry	Created
https://ftp.service-invest...		91.216.107.198	LIGNE WEB SERVICES - LWS	06.01.2020
https://shulovmarket.xyz...		72.9.152.26	XYZ.COM LLC	06.01.2020
https://paypalllimited.ser...		67.207.91.187	TLDS L.L.C. d/b/a SRSPlus	05.01.2020
https://paypalllimited.serveirc.com/signin/login.php		177.52.181.15	Churrascaria Mein Haus Ltda - ...	05.01.2020
https://saradesh24live.c...		198.54.116.167	NameCheap, Inc.	05.01.2020
https://ytmp3converts.c...		199.188.206.58	GoDaddy.com, LLC	04.01.2020
https://paypal.re		52.58.78.16	TLD Registrar Solutions Ltd	04.01.2020
http://paypal-198390927...		81.88.52.22	Register SPA	04.01.2020
http://vire0002.000web...		145.14.144.90	Hostinger, UAB	03.01.2020

Threat Intelligence for Leadership and Decision Makers

- Helps identifying and understanding the nature of the risk including emerging threats
  - Which attacks are becoming more/less frequent
  - Which kind of threat actors are expected
  - Which assets are most targeted

➔Optimized investments to enhance defensive measures

My Course on « Cybrary.it »

THANK YOU