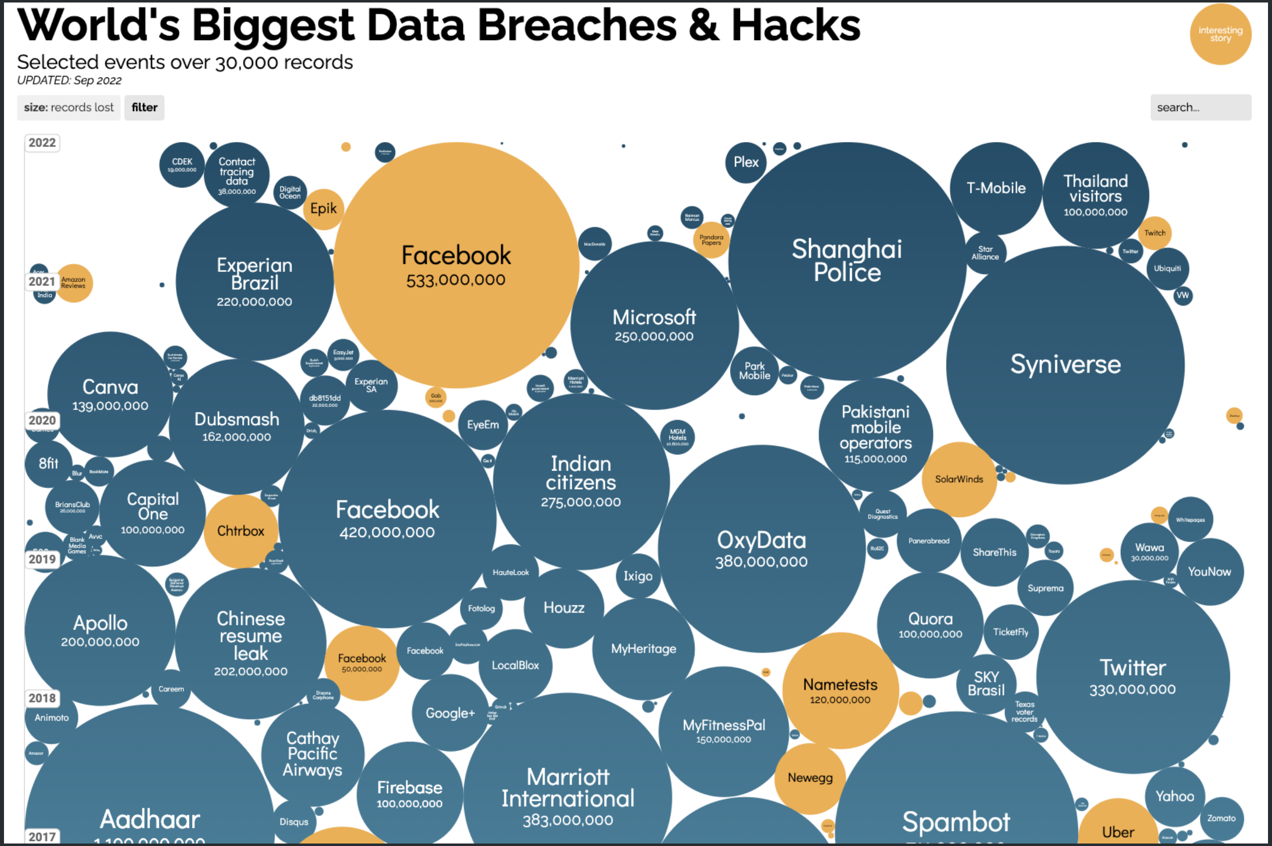
Increasing Threat of Cyber Attack

- Who is being attacked?
- Who is conducting the attack?
- Why are they attacking?
- What techniques are the adversaries using?
- Deeper dive on Ransomware
- How are their techniques evolving?
- What steps can be taken to address the risk?
- Who are IronNet and C-Stem

Who is being attacked



World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022

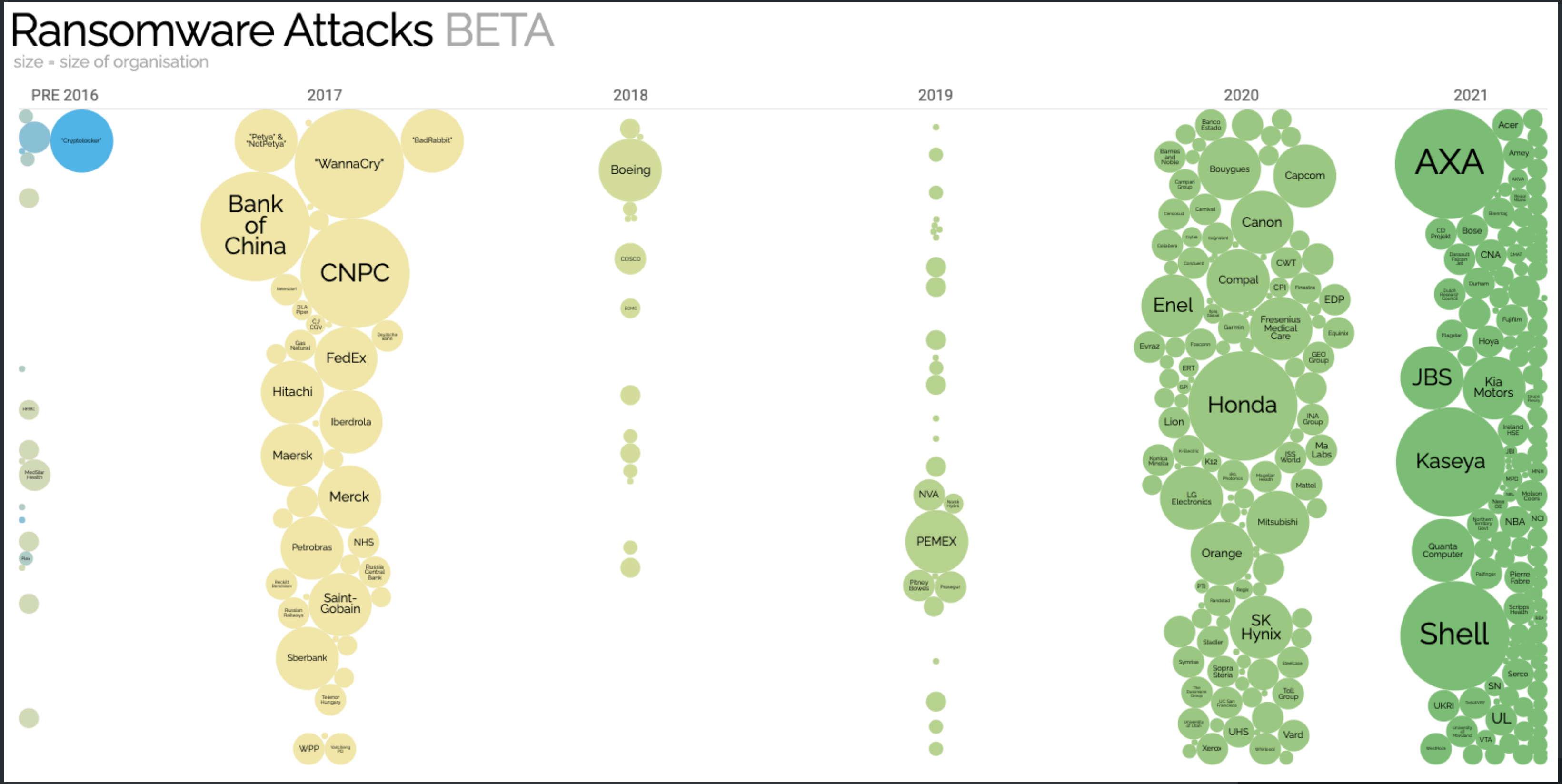
No geographical limitation

No Industry limitation

No restriction on victim size

Data from InformationisBeautiful.net

Who is being attacked (cont)



Data from InformationisBeautiful.net

Who is conducting the attacks?

Why are they attacking? What is the motivation?

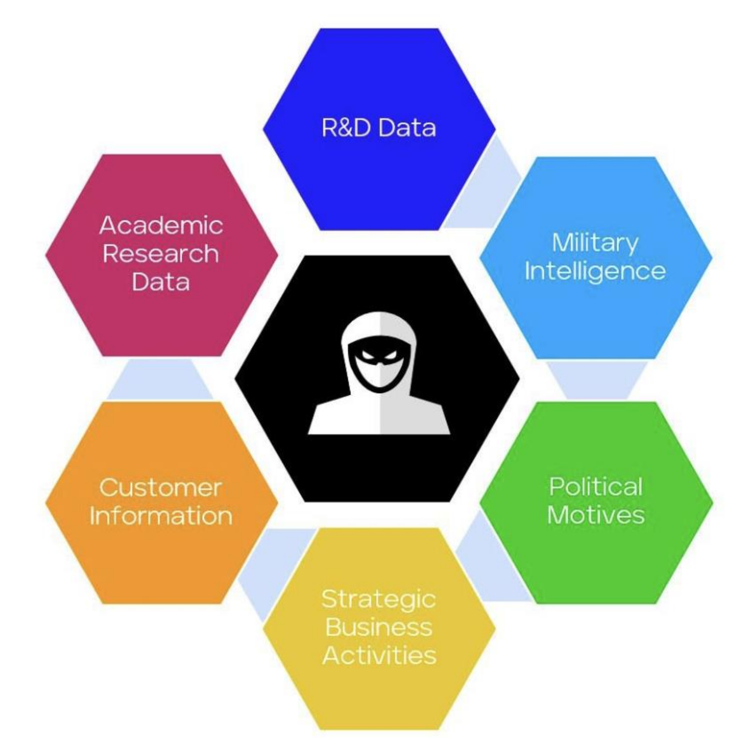
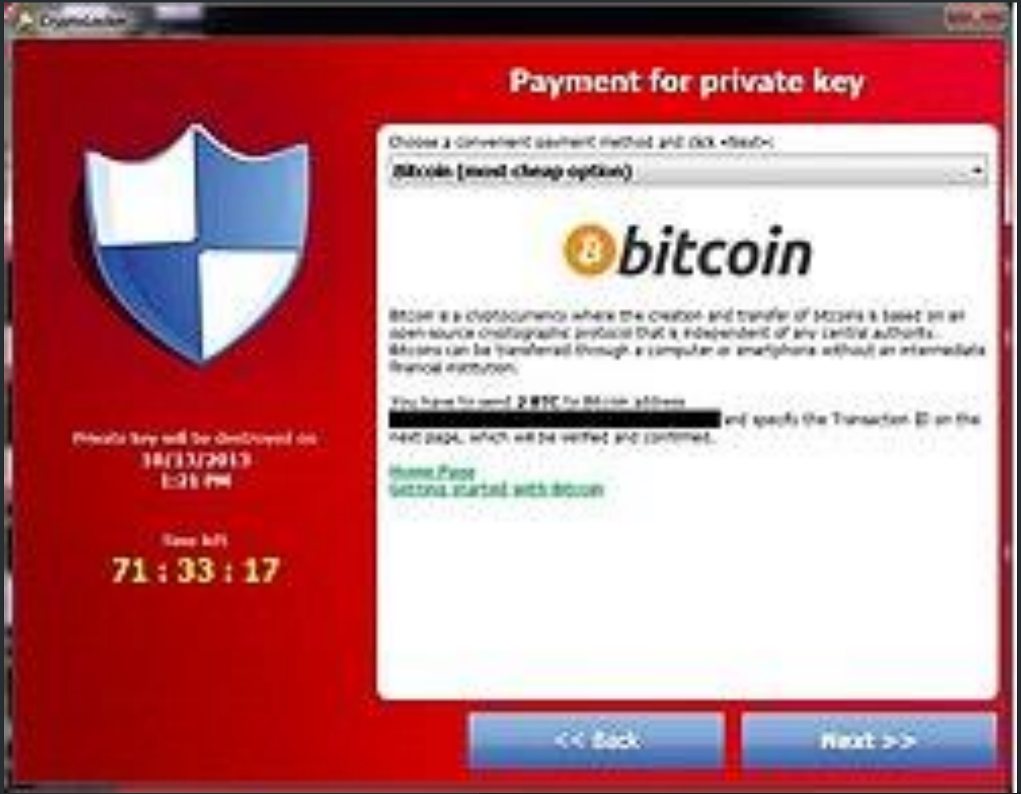


Figure 1: Cyber Espionage Key Targets

Image Source: Trellix Operation Graphite



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with bitcoin

Private key will be destroyed on
10/11/2013
1:21 PM

Time left
71 : 33 : 17

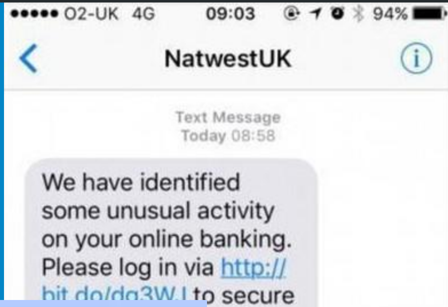
Image Source: Wikipedia Cryptolocker

What techniques are the adversaries using?

Phishing

Spear Phishing

Drive by Download

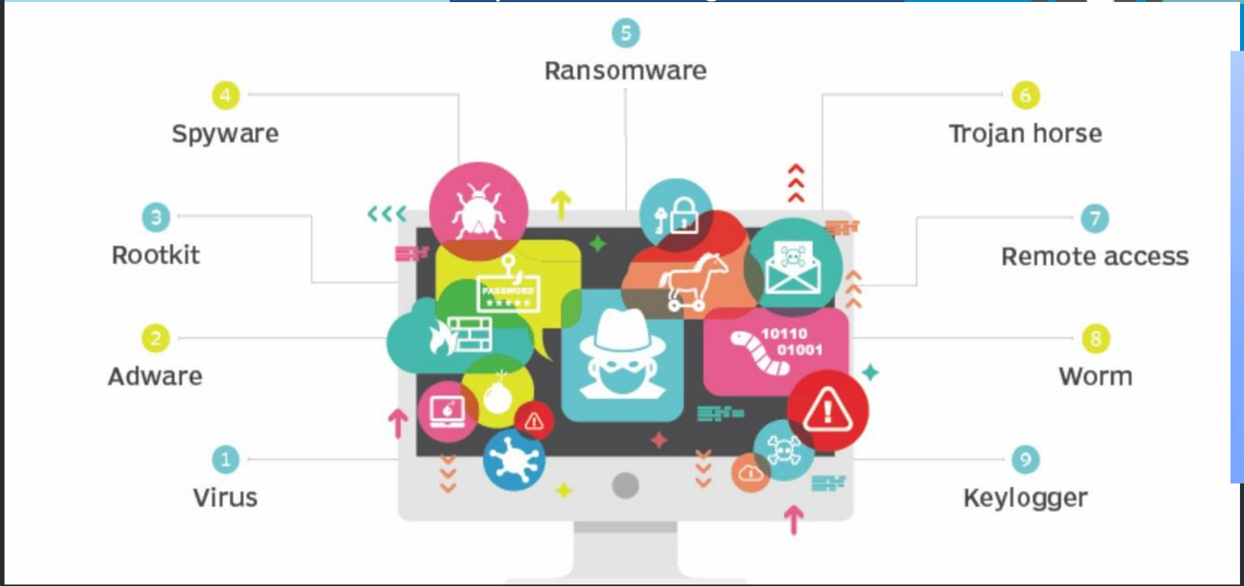


●●●●● O2-UK 4G 09:03 94%

NatwestUK

Text Message
Today 08:58

We have identified some unusual activity on your online banking. Please log in via http:// bit.do/dq3WJ to secure



5 Ransomware

4 Spyware

6 Trojan horse

3 Rootkit

7 Remote access

2 Adware

8 Worm

1 Virus

9 Keylogger

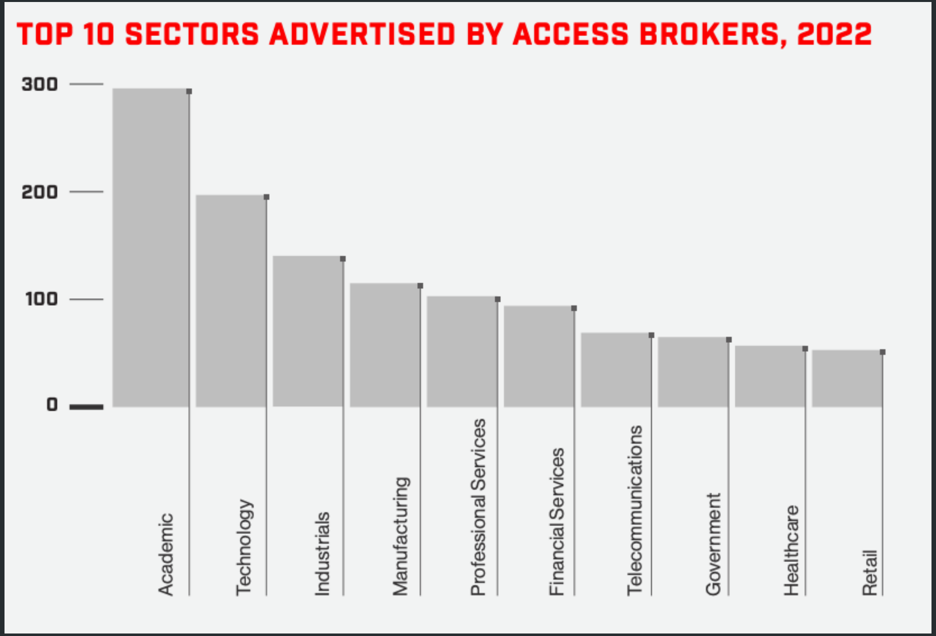
Image credits:
Malwarebytes
LinkedIn
NordVPN
Emisoft
Imagine IT

Ransomware Trends

- Mandiant: Investigations involving ransomware decreased by 15% from 2021 to 2022
- Crowdstrike: Average ransom demand dropped by around 28% from $5.7 million in 2021 to $4.1 million in 2022.
- Chainanalysis: Ransom payments decreased by 40% to $457 million.
- Factors influencing decline:
    - Ongoing disruption efforts targeting ransomware services and individuals
    - Drop in the value of cryptocurrencies like Bitcoin
    - Ukraine-Russia War impacts cybercriminal ecosystem
    - Cyber insurance companies setting restrictions
    - Actors needing to adjust their TTPs to adjust to global changes, such as Microsoft Office macros being disabled by default

Ransomware Trends

The Rise of Initial Access Brokers (IABs)



Crowdstrike

- In 30% of incidents investigated by Mandiant in Q4, the threat actors obtained access from a separately tracked threat cluster.
- In 2022, there was 112% increase in IAB ads, with more than 2,500 advertisements for access identified (by Mandiant)
- Recorded Future observed 3x the Dark Web listings for network access than it did in 2021
  - Bulk vs. one-access, one-auction
  - Increased use of infostealers
  - Spike in IAB market after Russia's invasion?
- 2022 saw continued shift away from using malware to gain initial access and persistence - malware-free activity accounted for 71% of all detections in 2022 (up from 62% in 2021).

Ransomware Trends

Group

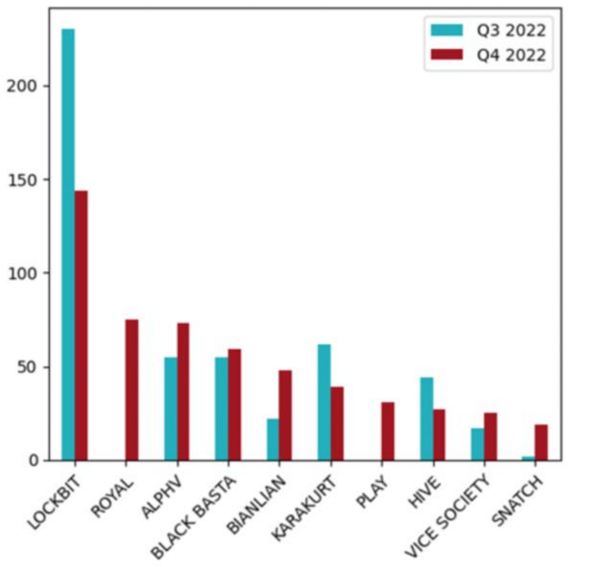
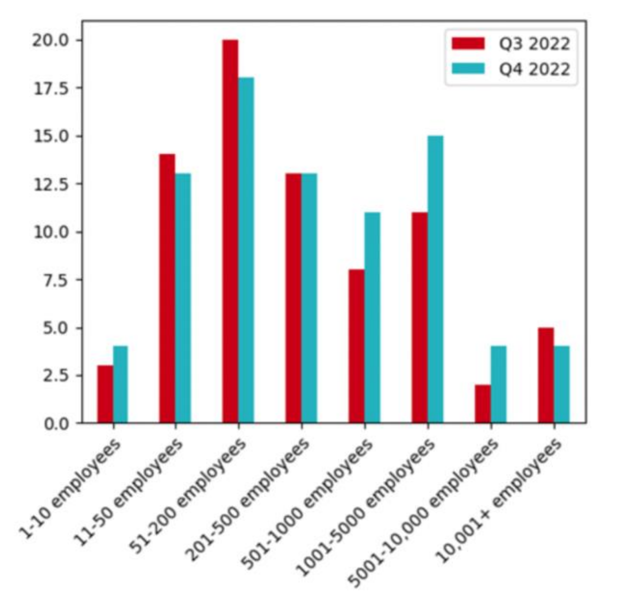


Figure 3: Number of DLS postings

Mandiant

Company Size



Mandiant

Region

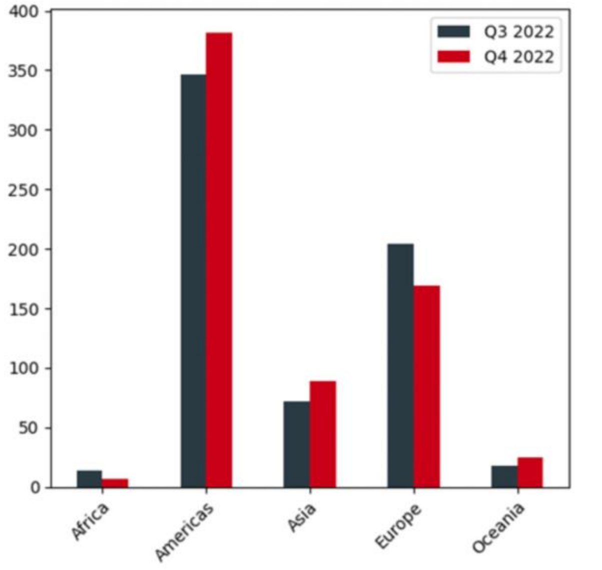


Figure 5: Number of DLS victims by region

Mandiant

Ransomware Trends

- Movement toward extortion without ransomware
  - Advantage -
    - Decrease reliance on ransomware - less chance of ransomware failing or being detected by security software
    - Less chance of disruption that would invoke retaliation
  - Con -
    - Need to dwell on victim infrastructure without being detected for long enough to identify and exfiltrate sensitive data
  - Extortion groups have a different targeting rationale than ransomware groups - focusing on large orgs with valuable data instead of opportunistic attacks

Industry

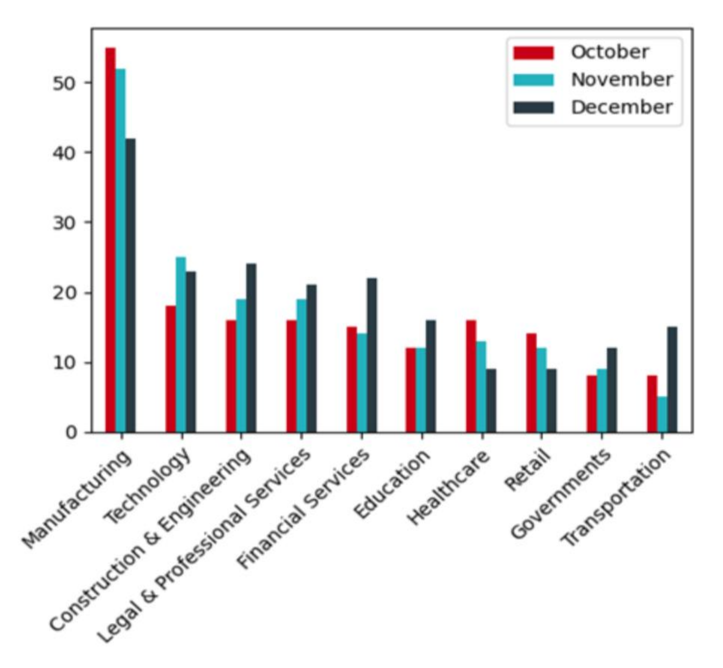
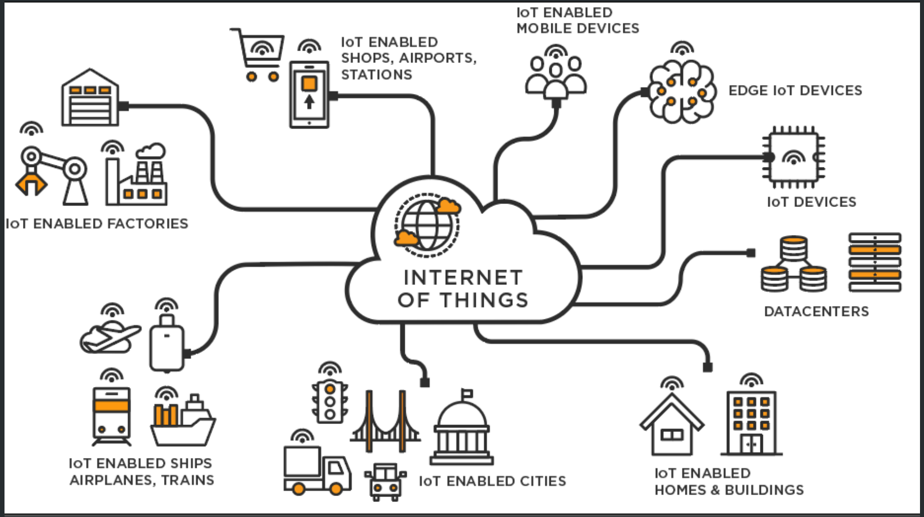


Figure 7: Number of DLS victims by industry

Mandiant

IABs for IoT


IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT DEVICES
IoT ENABLED FACTORIES
INTERNET OF THINGS
DATACENTERS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

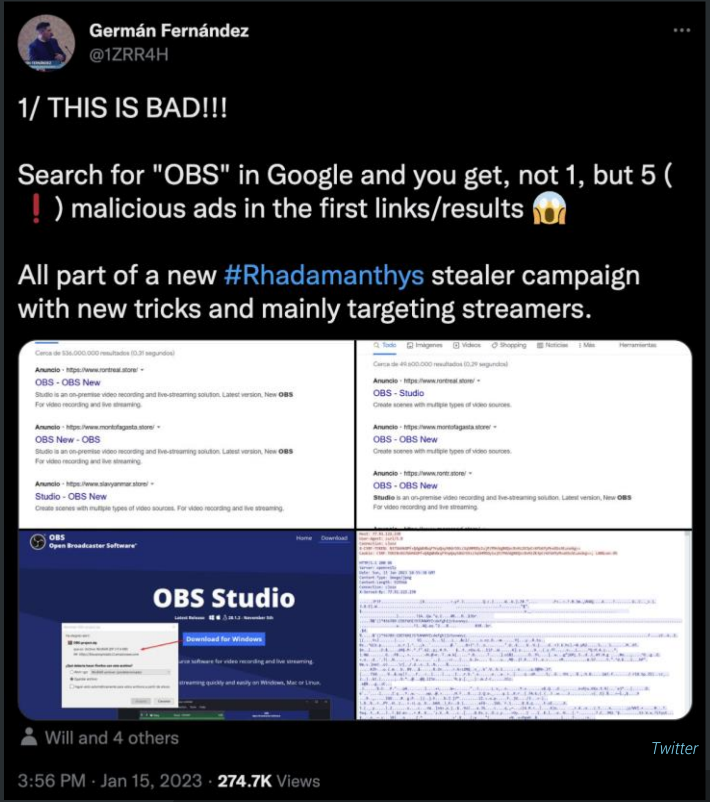
Michigan Ross

- IAB = Initial Access Broker / IoT = Internet of Things (any sort of device that connects to the internet).
- 3 main reasons IoT devices are vulnerable to attack:
    - Often used with default configurations
    - Patch management is difficult
    - IoT devices not designed with security in mind
- Many examples of APTs that have used corporate IoT for initial access into organizations, as well as cybercriminals.
- There are groups that trade IoT exploits on Dark Web markets – the logical next step is an IAB market for IoT.

TRENDS

Fake Software **& Google Ads**

- Rhadamanthys Stealer
  - New stealer discovered being sold as a MaaS and is being actively deployed
  - Spreads by using Google Ads that redirect the user to phishing websites that mimic popular software such as Zoom, AnyDesk, Notepad++, Bluestacks, etc.
- Rhadamanthys is just one example of a larger trend – there have been many other incidents lately where cybercriminals abused Google Ads.
  - Google pay-per-click ads spreading IcedID
  - 1,300 domains impersonate AnyDesk to spread Vidar Stealer
  - Royal ransomware and Batloader deployed through Google ads and malvertising



Germán Fernández
@1ZRR4H

1/ THIS IS BAD!!!

Search for "OBS" in Google and you get, not 1, but 5 (❗) malicious ads in the first links/results 😱

All part of a new #Rhadamanthys stealer campaign with new tricks and mainly targeting streamers.

Cerca de 536.000.000 resultados (0,31 segundos)

Anuncio · https://www.rontreal.store/
OBS - OBS New
Studio is an on-premise video recording and live-streaming solution. Latest version, New **OBS** For video recording and live streaming.

Anuncio · https://www.montofagasta.store/
OBS New - OBS
Studio is an on-premise video recording and live-streaming solution. Latest version, New **OBS** For video recording and live streaming.

Anuncio · https://www.slavyanmar.store/
Studio - OBS New
Create scenes with multiple types of video sources. For video recording and live streaming.

Cerca de 49.600.000 resultados (0,29 segundos)

Anuncio · https://www.rontreal.store/
OBS - Studio
Create scenes with multiple types of video sources.

Anuncio · https://www.montofagasta.store/
OBS - OBS New
Create scenes with multiple types of video sources.

Anuncio · https://www.rontr.store/
OBS - OBS New
Studio is an on-premise video recording and live-streaming solution. Latest version, New **OBS** For video recording and live streaming.

Will and 4 others

Twitter

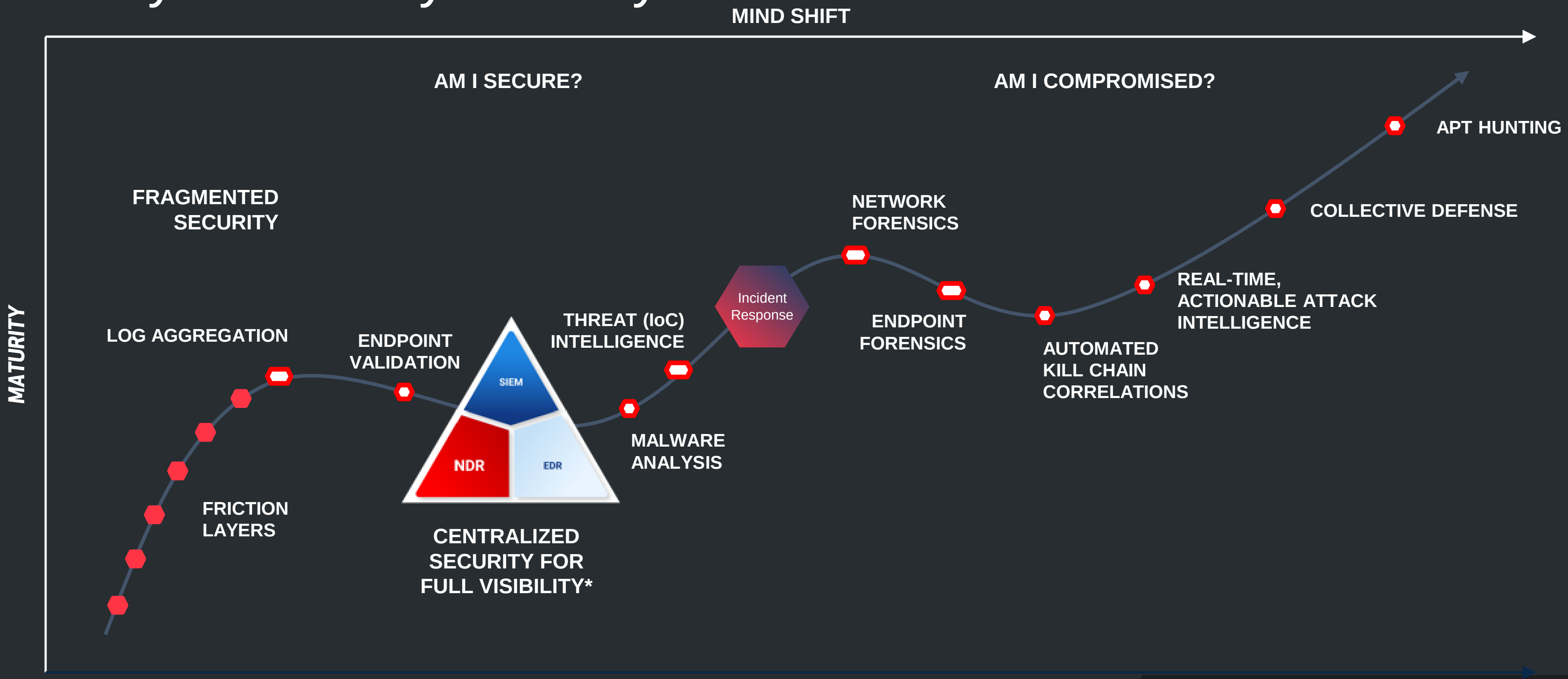
3:56 PM · Jan 15, 2023 · **274.7K** Views

ChatGPT **& AI**

- ChatGPT being used by cybercriminals to improve and build malware and ransomware
  - Numerous underground hacking forums in which cybercriminals discuss creating infostealers, encryption tools, and other malware - with the help of ChatGPT.
  - Make more convincing phishing campaigns by cutting out human error
  - Also using it to build supporting software, like a dark web marketplace
- ChatGPT lowering the barrier to entry into cybercrime?
  - Has potential to speed up the process for hackers by giving them a good starting point.

Slate

Cybersecurity Maturity



MIND SHIFT

AM I SECURE?

AM I COMPROMISED?

MATURITY

FRAGMENTED SECURITY

LOG AGGREGATION

FRICTION LAYERS

ENDPOINT VALIDATION

CENTRALIZED SECURITY FOR FULL VISIBILITY*

THREAT (IoC) INTELLIGENCE

MALWARE ANALYSIS

NETWORK FORENSICS

ENDPOINT FORENSICS

AUTOMATED KILL CHAIN CORRELATIONS

REAL-TIME, ACTIONABLE ATTACK INTELLIGENCE

COLLECTIVE DEFENSE

APT HUNTING

> “While in government, we saw attacks that could have been prevented if companies had the ability to work together collectively in real-time to share insights and to collaborate on defenses.”

IronNet was created to fill that void.

GEN (Ret.) Keith Alexander
Founder and Co-CEO, IronNet
Former Director of the NSA and U.S. CYBERCOM

IronNet

ESTEM