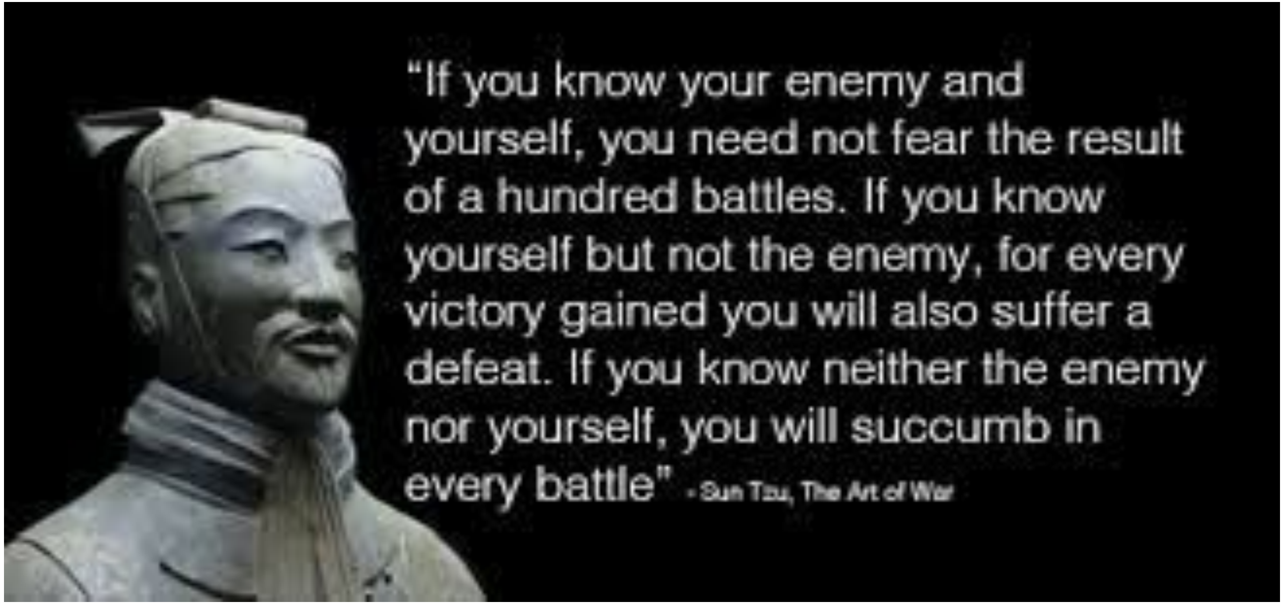
The Importance of Intelligence and Identity in Cybersecurity

Patrick Gardner
https://www.linkedin.com/in/patrick-a-gardner/

Why do we need threat intelligence?



"If you know your enemy and yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle" - Sun Tzu, The Art of War

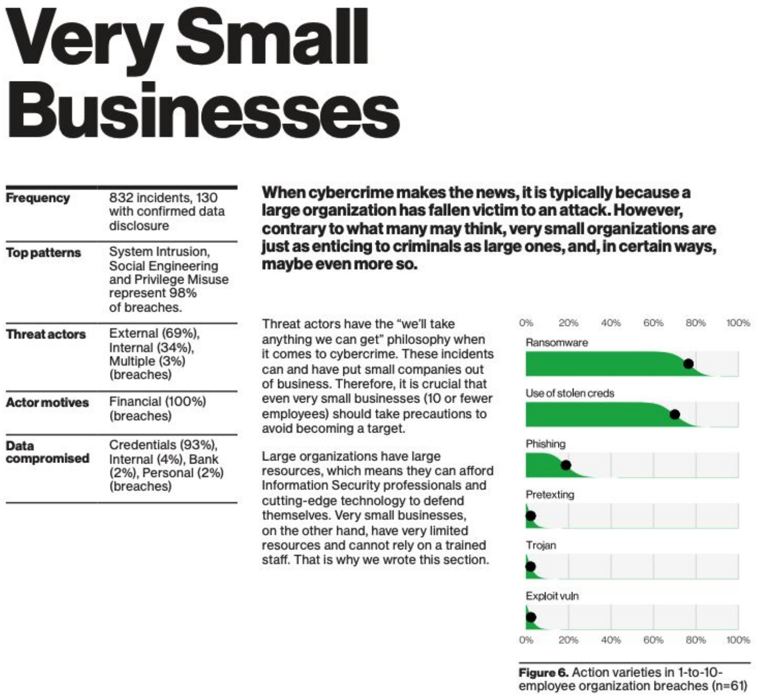
To defend well, you have to know the adversary

What are some examples of intelligence?

- Cyber Threat Intelligence (CTI)
  - Deep/darkweb forums and communities
  - Card shops
  - Ransomware
- Vulnerabilities and Exploits
- Fraud
- Stolen Credentials and Identities
- Geospatial intelligence
- Adversary Intelligence (APT, Criminal Organizations, General Botnets/Cybercrime, Hacktivism)
- OSINT (Open Source Intelligence - Data from publicly available sources)

But does this really apply to me? I am not a bank, government, or large business!

- With Ransomware and supply chain attacks, you better believe it does!



Very Small Businesses

Frequency	832 incidents, 130 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Privilege Misuse represent 98% of breaches.
Threat actors	External (69%), Internal (34%), Multiple (3%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Credentials (93%), Internal (4%), Bank (2%), Personal (2%) (breaches)

When cybercrime makes the news, it is typically because a large organization has fallen victim to an attack. However, contrary to what many may think, very small organizations are just as enticing to criminals as large ones, and, in certain ways, maybe even more so.

Threat actors have the "we'll take anything we can get" philosophy when it comes to cybercrime. These incidents can and have put small companies out of business. Therefore, it is crucial that even very small businesses (10 or fewer employees) should take precautions to avoid becoming a target.

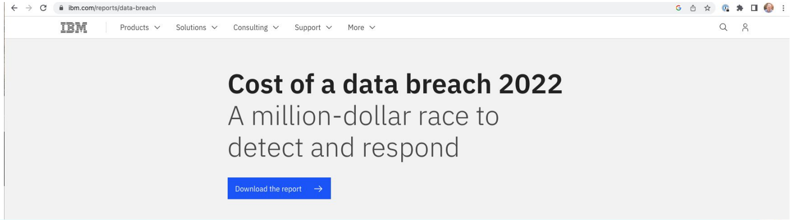
Large organizations have large resources, which means they can afford Information Security professionals and cutting-edge technology to defend themselves. Very small businesses, on the other hand, have very limited resources and cannot rely on a trained staff. That is why we wrote this section.

Figure 6. Action varieties in 1-to-10-employee organization breaches (n=61)

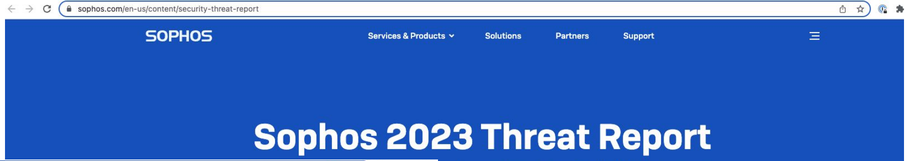
Source Verizon DBIR: https://www.verizon.com/business/resources/T21c/reports/2022-dbir-smb-snapshot.pdf

There are a LOT of free useful reports to understand the landscape

- Some good examples include Verizon Data Breach Investigations Report, IBM Data Breach Report, Crowdstrike Global Threat Report, Sophos Security Threat Report



Cost of a data breach 2022
A million-dollar race to detect and respond



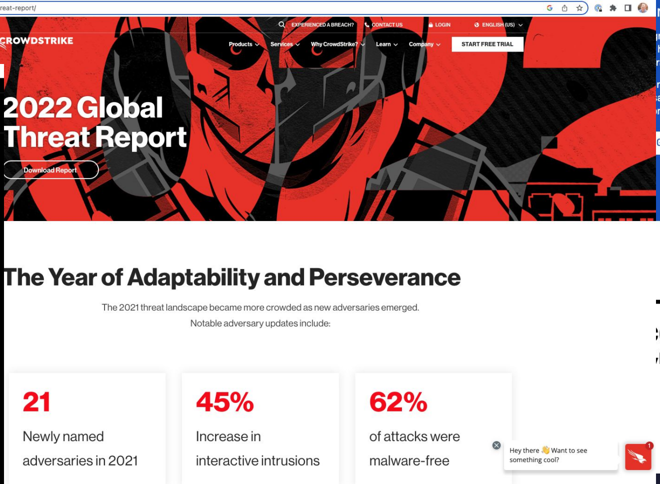
Sophos 2023 Threat Report

malware "as-a-service" global economy

roups spread misinformation and launched multiple cyberattacks against Ukraine, hardware security products made by nearly every company in the cybersecurity and rastructure industries.

nsformed into an industry. Information technology companies have shifted to "as-a-ame. Access brokers, ransomware, information-stealing malware, malware delivery, ns have lowered barriers to entry for would-be cybercriminals.

-service continues to onomic landscape of



2022 Global Threat Report

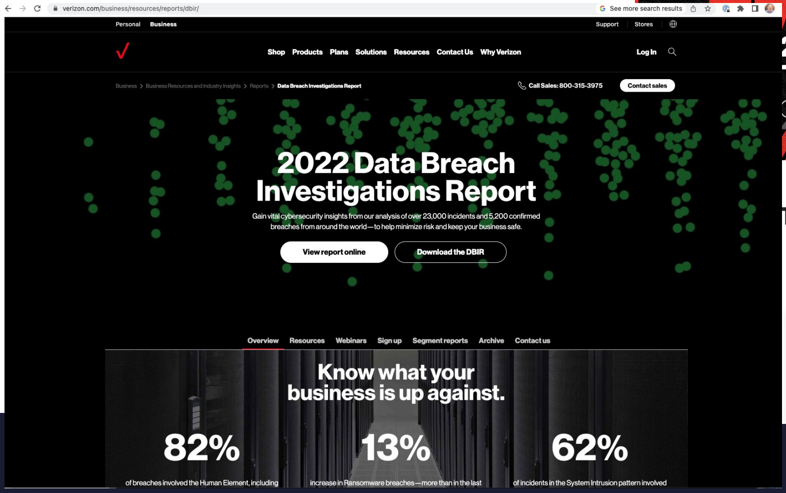
The Year of Adaptability and Perseverance

The 2021 threat landscape became more crowded as new adversaries emerged. Notable adversary updates include:

21 Newly named adversaries in 2021

45% Increase in interactive intrusions

62% of attacks were malware-free



2022 Data Breach Investigations Report

Gain vital cybersecurity insights from our analysis of over 23,000 incidents and 5,200 confirmed breaches from around the world—to help minimize risk and keep your business safe.

Know what your business is up against.

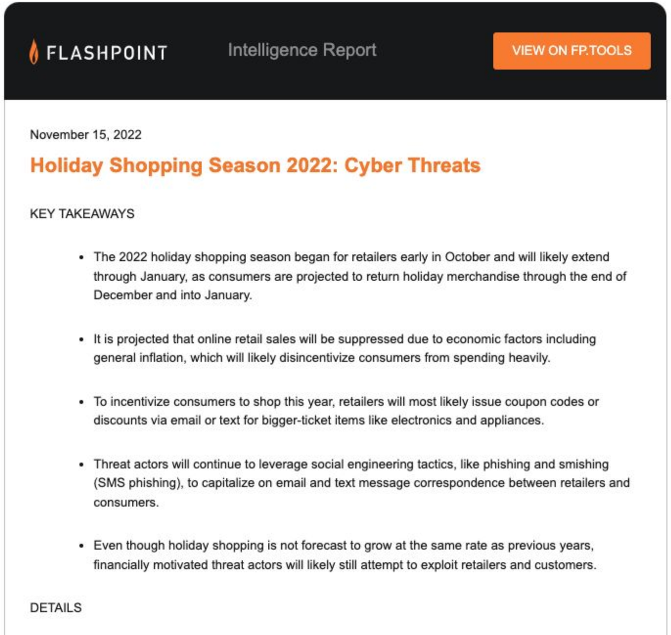
82% of breaches involved the Human Element, including

13% increase in Ransomware breaches—more than in the last

62% of incidents in the System Intrusion pattern involved

As your security needs grow, there are number of commercial Intelligence offerings

- These solutions give you specific and targeted intel that is directly actionable
- These companies specialize in the Intel Cycle and tradecraft
- As a customer you get access to finished intelligence reports, curated alerting, custom research, and direct access to the intel data to drill in



FLASHPOINT Intelligence Report VIEW ON FP.TOOLS

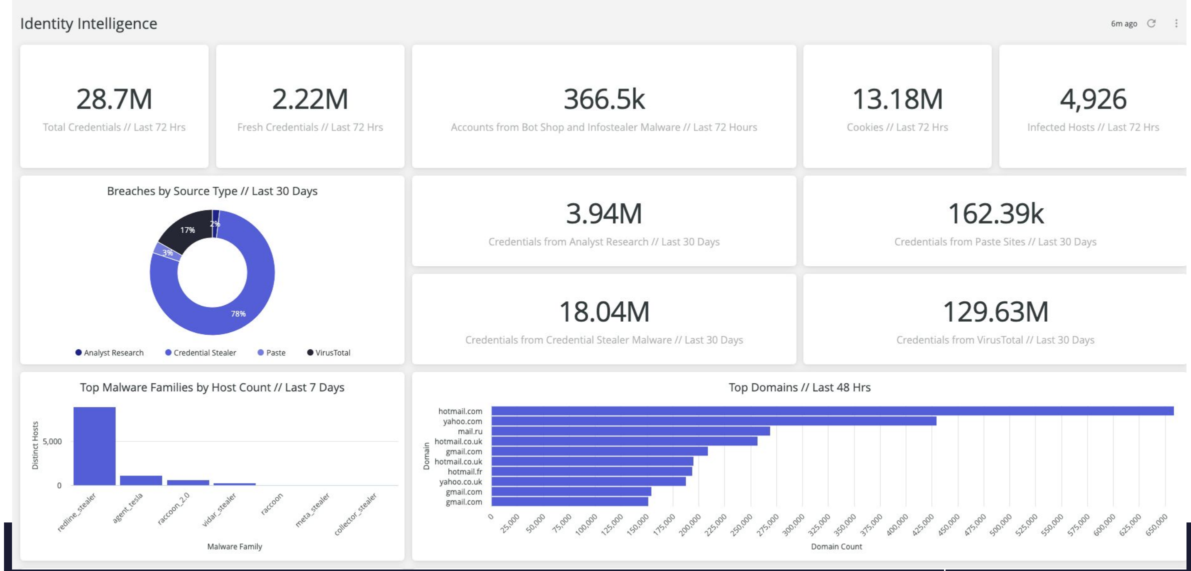
November 15, 2022

Holiday Shopping Season 2022: Cyber Threats

KEY TAKEAWAYS

- The 2022 holiday shopping season began for retailers early in October and will likely extend through January, as consumers are projected to return holiday merchandise through the end of December and into January.
- It is projected that online retail sales will be suppressed due to economic factors including general inflation, which will likely disincentivize consumers from spending heavily.
- To incentivize consumers to shop this year, retailers will most likely issue coupon codes or discounts via email or text for bigger-ticket items like electronics and appliances.
- Threat actors will continue to leverage social engineering tactics, like phishing and smishing (SMS phishing), to capitalize on email and text message correspondence between retailers and consumers.
- Even though holiday shopping is not forecast to grow at the same rate as previous years, financially motivated threat actors will likely still attempt to exploit retailers and customers.

DETAILS



Identity Intelligence

6m ago

28.7M
Total Credentials // Last 72 Hrs

2.22M
Fresh Credentials // Last 72 Hrs

366.5k
Accounts from Bot Shop and Infostealer Malware // Last 72 Hours

13.18M
Cookies // Last 72 Hrs

4,926
Infected Hosts // Last 72 Hrs

3.94M
Credentials from Analyst Research // Last 30 Days

162.39k
Credentials from Paste Sites // Last 30 Days

18.04M
Credentials from Credential Stealer Malware // Last 30 Days

129.63M
Credentials from VirusTotal // Last 30 Days

Breaches by Source Type // Last 30 Days

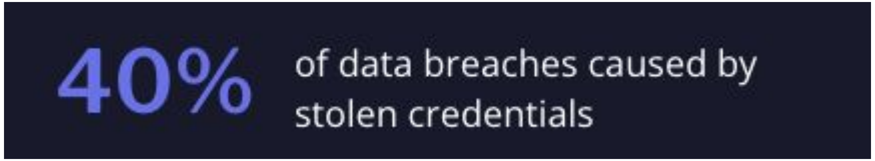
Top Malware Families by Host Count // Last 7 Days

Top Domains // Last 48 Hrs

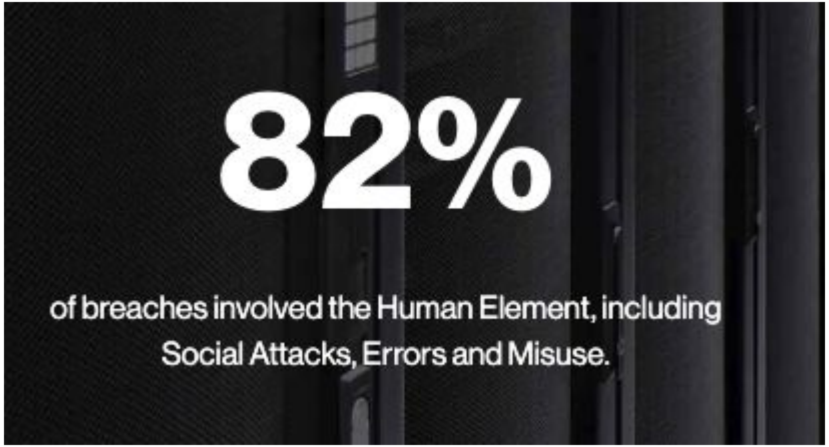
Speaking of Identity…

Identity is increasingly the attack vector of choice

- Examples of identity based attacks include Phishing, Smishing (SMS Phishing), password reuse, and compromised/stolen credentials



40% of data breaches caused by stolen credentials



82%

of breaches involved the Human Element, including Social Attacks, Errors and Misuse.

Source Verizon DBIR

Identity in your IT and Security Strategy

- Without a good Identity and access management (IAM) plan, you will be compromised
- Know how you authenticate and grant access to all your resources
  - Think about all your SaaS products and contractors/vendors
- Best practices
  - Use a Federated Identity provider and SSO to centralize access control
  - Enforce strong passwords and MFA
  - Use a password vault
  - Monitor IAM activities and look for anomalies, reply attacks, logins from different geographies, etc
  - Regularly review and trim accounts and access for departed employees, vendors, etc

Thank You!