Predictive Cyber Defense

Early Warning Intelligence & Forecasting

Whoami?

- Red Team Lead @ HelloFresh
- Member of Curated Intel

Twitter : @1ce7ea
LinkedIn : linkedin.com/in/robin-dimyan/
Website : robindimyan.medium.com

Program Agenda

1. What is Predictive Defense?
2. Predictive Analysis Techniques
3. Early Warning System
4. Forecasting Cyber Crime
5. Geopolitical Cyber Risk Analysis

Reactive vs. Proactive vs. Predictive Defense

Reactive:

- The attack ***has started*** and we might be a potential target.

Proactive:

- The attack ***hasn't started yet***, but it might target us when it does.

Predictive:

- The attack is ***expected to start within a certain time frame*** and we could be a target.

Predictive Analysis Techniques

1. Indications and Warnings Analysis
2. Cone of Plausibility
3. Signpost Analysis
4. Correlation-based Techniques
5. Bayesian Probability

Research Questions

“How can I detect the upcoming spear-phishing attacks?”

“How can I identify the vulnerabilities that are most likely to be exploited in the wild?”

“How can I predict what kind of threats will be more relevant to me in the future?”

“How can I foresee the development of a cyber crime market which targets my organization?”

Research Questions

“How can I detect the upcoming spear-phishing attacks?”

➡ Are there any early signs of a spear-phishing campaign that I can observe?

“How can I identify the vulnerabilities that are most likely to be exploited in the wild?”

➡ What factors are influential in adoption of a vulnerability by the attackers?

“How can I predict what kind of threats will be more relevant to me in the future?”

➡ What influences targeting decisions by the adversaries?

“How can I foresee the development of a cyber crime market which targets my organization?”

➡ What drives a change in the TTPs of adversaries?

EARLY WARNING SYSTEM

Introduction to Research Methodologies

Research Approaches

1. Profile-driven research

- You profile certain attack types or campaigns and use these patterns to predict future attacks.

2. Correlation-guided research

- You look for correlations between different events and attack types without profiling.
- Then, you investigate any correlation you have found to construct your hypothesis.

Profile-driven Research

Case study: Spear-phishing attacks

Spear-phishing Attacks

An adversary's possible preparation steps for a spear-phishing attack:

- Curating a list of employees to be targeted
  - Scraping public websites, LinkedIN etc.
  - **Interrogating the identity services (Azure-AD, LDAP etc.)**
  - **Interrogating the email server/provider**
- Setting up the phishing infrastructure
  - **Malware host / landing page**
  - **Staging and C2 servers**
  - **Domain names, SSL certs**
- Setting up the distribution method
  - Bulk email services (Mailchimp etc.)
  - Self-hosted email server
  - Known email providers (Gmail etc.)

Profiling the Spear-phishing Attacks

Defender's perspective

Look for patterns in the phishing instances you received. It doesn’t have to be a single pattern across all instances, you will probably have multiple clusters.

- ➡ What is the mean time between two spear-phishing attacks?
- ➡ What is the distribution of these attacks throughout the year?
- ➡ How many employees are targeted in each cluster?
- ➡ Which malware families do I receive through these phishings?
- ➡ What do landing pages look like? Is it possible to fingerprint them?

Example: Leery Turtle Campaigns

Spear-phishing campaigns targeting crypto-exchange businesses worldwide that are later attributed to North Korea.

- Domain names used in Leery Turtle campaigns contain at least two of the following words: google, drive, cloud, share, upload.
- Leery Turtle staging servers had ports 80 and 8080 open at the same time because they were compromised web apps.
- There were approx 3 months between two campaigns

These patterns have remained consistent for at least two years!

Reference: https://github.com/robindimyan/Publications/blob/master/LeeryTurtle%20Quick%20Analysis.pdf

I&W Analysis

Mail / Identity servers

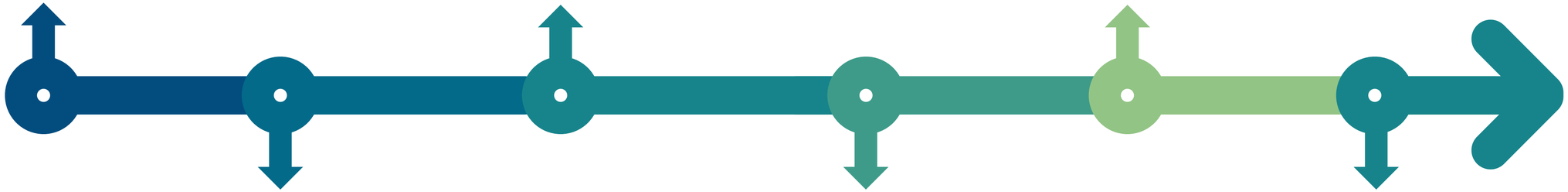
Monitor for interrogation of your identity/email services.

Infrastructure pivoting

New domains fitting the pattern
New servers with similar config

Vendor reports / OSINT

Recent reports of the same campaign that are of interest



New infrastructure

Scan the internet to spot new infrastructure based on the profiles

New malware samples

Monitor malware families that are of interest using open sources

Campaign start

Building the Early Warning System

Data analysis!

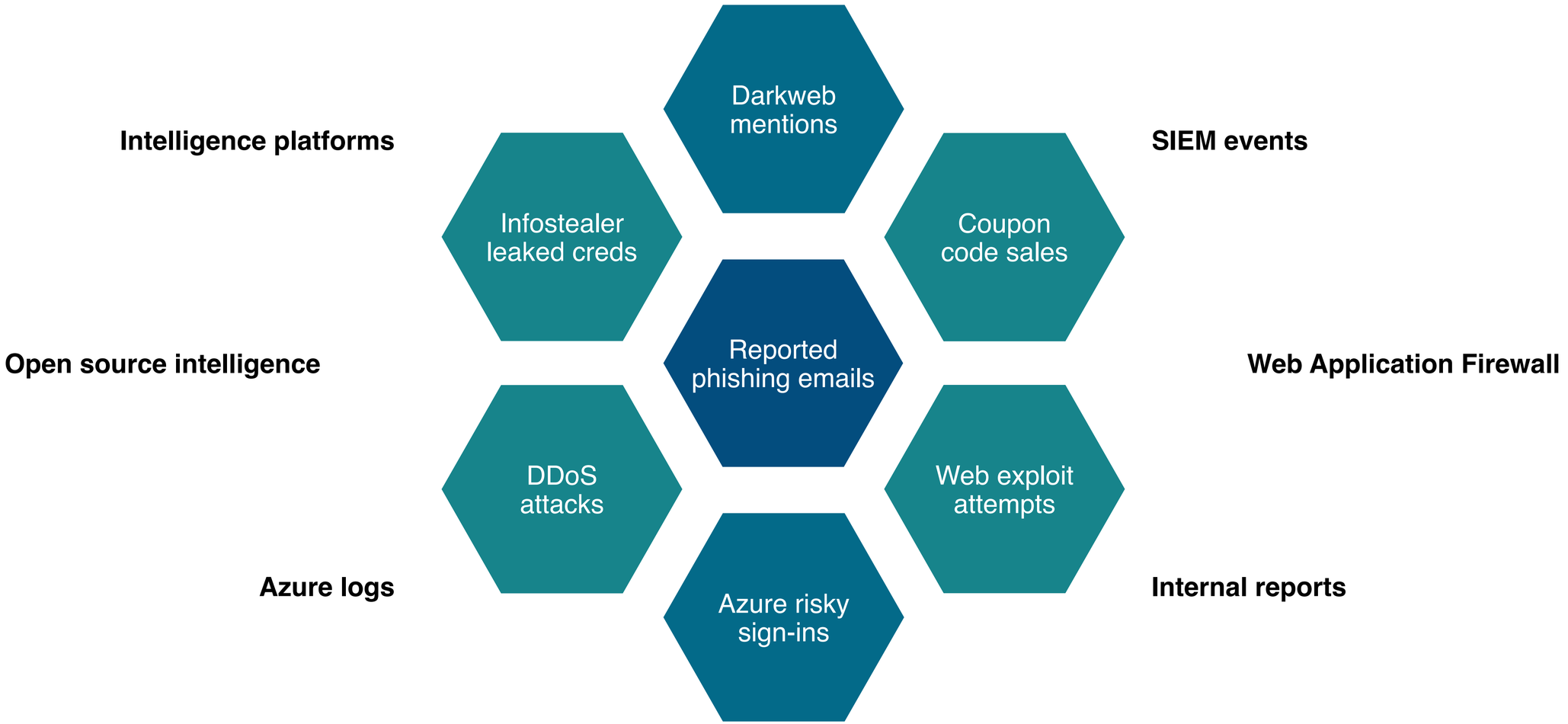
- Extract a history of these signals retrospectively (if possible)
- Compare with the history of spear-phishing attacks you have received
- Try different weights and combinations to see which model makes the best prediction
- You can use mean-time between two attacks as the signal lifetime
  - You can also use mean-time between attacks to schedule threat hunts!
- Sometimes the model is not good enough, so you may have to start over

Reference: https://robindimyan.medium.com/early-warning-intelligence-how-to-predict-cyber-attacks-1299af2dada3

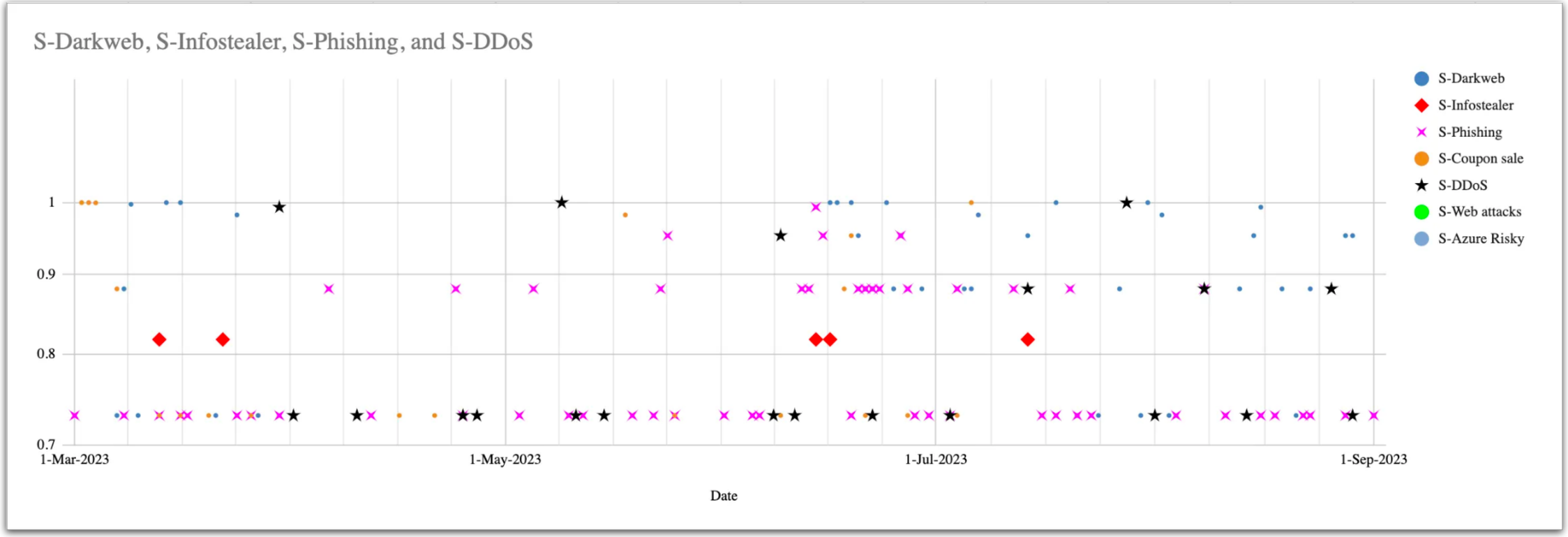
Correlation-guided Research

Case study: Infostealers and credential stuffing

Collecting Data



Correlation-guided Research



Reference: https://robindimyan.medium.com/how-to-build-early-warning-system-with-examples-692b66fa73d6

Correlation-guided Research

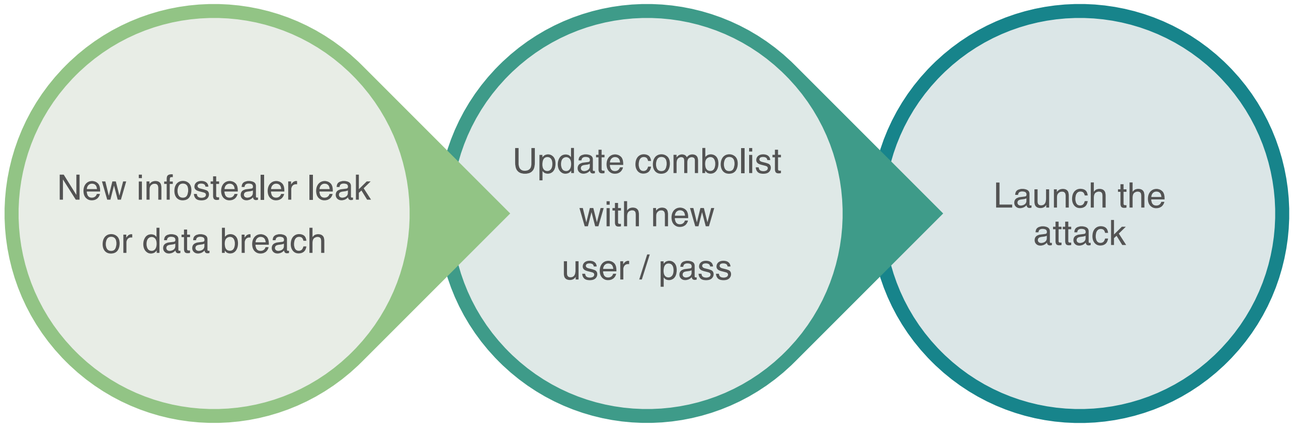
The second step is to filter out data sets with low variation among them.

- An event that occurs almost every day renders any correlation with itself meaningless.

Afterward, the binary combinations of these events are compared using a correlation function.

	C-Info/Darkweb	C-Info/Phishing	C-Info/Coupon	C-Info/DDoS
t - 0w	0.09185235584	0.1625176389	0.1176877883	0.09176629355
t - 1w	0.044535426	0.02222222222	0.2953721743	-0.07352146221
t - 2w	-0.06565321643	0.2311113647	0.1828275852	-0.417855447

Constructing the Hypothesis



If accounts belonging to our organization or our customers have been leaked in publicly shared Infostealer logs (and data breaches), there is a 40% probability that a DDoS/credential stuffing attack will occur within two weeks.

I&W Analysis

Infostealer and data breaches

Identify and monitor sources where Infostealer logs and data breaches are publicly shared

Identify customer accounts

Detect leaked accounts belonging to our organization and customers

Alerting

Generate alerts if the number of these compromised accounts exceeds a certain threshold

Key Takeaways

- Identifying early signs of an attack is possible if we focus on its preparatory stages.
- Developing early signals involves analysing internal data to understand the characteristics of cyber attacks and identifying patterns or correlations.
- A well-developed warning model using these signals can predict events with a degree of probability, giving defender teams ample time to prepare.

FORECASTING

Analytic Frameworks for Cyber Crime and Espionage

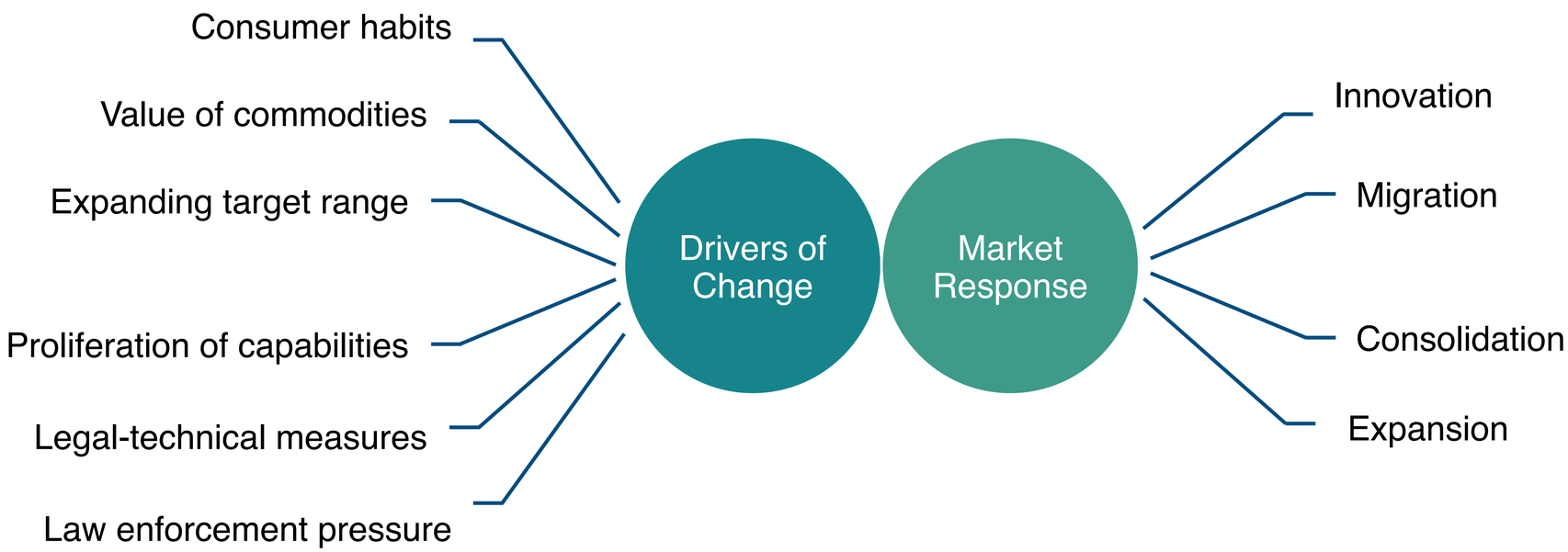
Forecasting

- Assessment of “what’s next?” in long term (1+ year)
- Ideally should inform security leadership decisions so the organization is better positioned against future threats.
- Some analytic frameworks from traditional intelligence analysis: PESTLE-M, DIMEFIL, STEMPLES+

Cyber Crime Forecasting

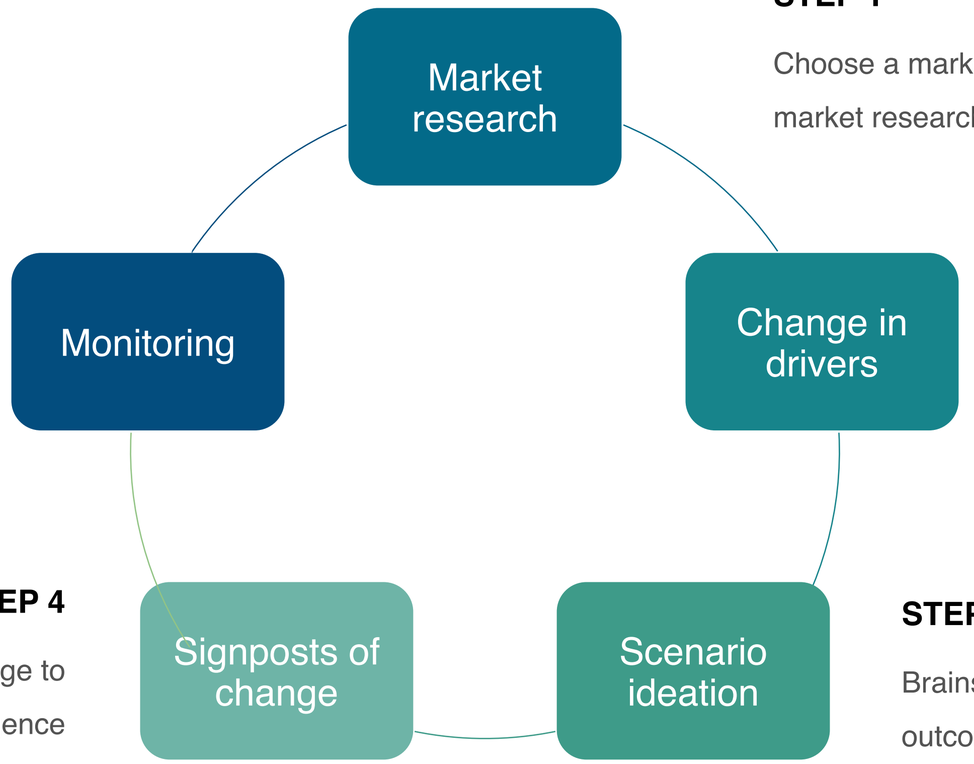
Analysing cyber crime markets by understanding its drivers

Cyber Crime Market Dynamics



Reference: https://robindimyan.medium.com/predictive-defense-how-to-do-cyber-crime-forecasting-with-examples-548c22e4a4e5

Cyber Crime Forecasting



STEP 1

Choose a market and conduct basic market research

STEP 2

Assess possible changes in the market drivers

STEP 3

Brainstorm scenarios for potential outcomes

STEP 4

Determine signposts of change to monitor for scenario emergence

STEP 5

Observe darkweb sources for emergence of scenarios

Credential Stuffing Market

Step 1: Choose a market and conduct basic market research

Basic intelligence requirements	Answers
How many successful trades are conducted within a certain time frame, if applicable?	An estimated 20,000 to 32,000 coupons/accounts are sold annually.
Estimated trade volume within a certain time frame, if applicable?	Estimated market volume: yearly $150,000 to $240,000.
Who are the consistent suppliers, if applicable?	The distribution of supply in the market is as follows: • 1 actor controls 25% • 5 actors account for another 25% • The remaining 50% is shared among 53 actors Thus, half of the total market volume is shared between just 6 actors. The other half is distributed among 53 smaller-scale actors.
Who are the major buyers, if applicable?	The commodities sold are products directed at end-users, like premium accounts and coupon codes. Hence, these products are mostly sold at retail, not wholesale.
What is the relationship between these people?	No direct relationship has been observed among the identified actors.

Cone of Plausibility

Step 2: Assess possible changes in the market conditions

Step 3: Brainstorm scenarios for potential outcomes of changed conditions

DRIVERS	QUESTION	ASSUMPTION	OUTCOME
Consumer habits	Is there a reason for consumer habits to change in the future?	Post the COVID-19 pandemic, there is a decrease in consumer demand for digital products and services.	With their source of income diminishing due to decreased customer demand, criminals migrate to other markets, such as initial access brokerage, where they can repurpose their skills. (migration)

Reference: https://robindimyan.medium.com/predictive-defense-how-to-do-cyber-crime-forecasting-with-examples-548c22e4a4e5

Cone of Plausibility

Drivers	Questions	Assumptions	Outcomes
Consumer habits	Is there a reason for consumer habits to change in the future?	Post the COVID-19 pandemic, there is a decrease in consumer demand for digital products and services.	Criminals will find a way to circumvent the CIAM and bot protections, and continue their attacks as usual. (**innovation**)
Value of commodity	Is there anything that might change the value of the commodity?	-	The profit margin for attacks substantially increases due to decreased infostealer log prices, leading to more players entering the market. (**expansion**)
Expanding target range	Can the same profits be acquired by diversifying targets?	-	With their source of income diminishing due to decreased customer demand, criminals migrate to other markets, such as initial access brokerage, where they can repurpose their skills. (**migration**)
Proliferation of capabilities	Could a product or service be developed that would further facilitate executing the attacks?	Infostealer logs are available at very cheap prices making them suitable for enhancing the effectiveness of credential stuffing attacks.	Due to the increasing difficulty of exploitation, the market will consolidate around a few players with high capabilities. (**consolidation**)
Legal & technical measures	Are there reasons that might increase interest from governments and companies in this type of attack in the future?	1. Privacy regulations is likely to call for enhanced protection against credential stuffing attack because of their impact on PII. 2. As CIAM and bot protection solutions gain more widespread adoption, executing credential stuffing attacks become more challenging.	Criminals will abandon the credential stuffing technique and shift their focus to exploiting application vulnerabilities for account takeover. (**innovation**)

Signpost Analysis

Step 4: Determine signposts of change to monitor for scenario emergence

With their source of income diminishing due to decreased customer demand, criminals migrate to other markets, such as initial access brokerage, where they can repurpose their skills. (**migration**)

Signposts of change:

- ➡ # of messages containing coupon sale related keywords decreases over time
- ➡ Known coupon retailers starts selling other commodities

Key Takeaways

- Financially motivated cyber crime is influenced by market-like forces of supply and demand.

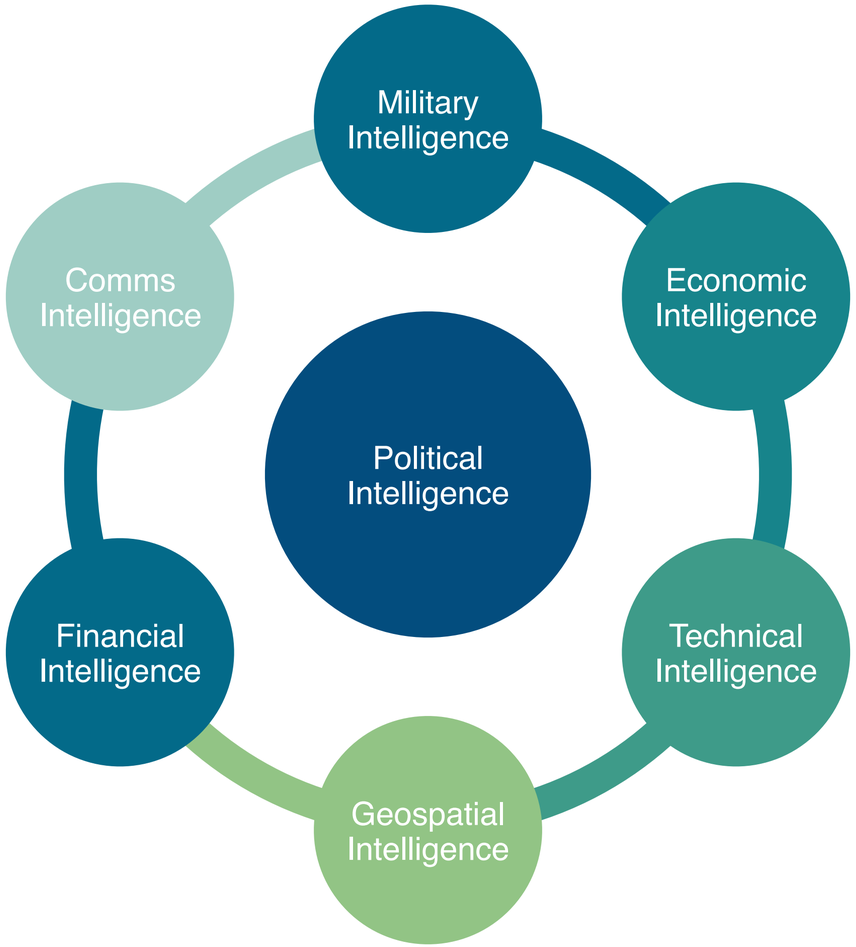
- It's essential to understand the factors driving supply and demand, like consumer behavior, commodity value, and legal and technical measures, to effectively analyse cyber crime markets.

- Markets react to changes in these conditions with patterns such as innovation, migration, consolidation, or expansion.

Geopolitical Cyber Risk Analysis

Understanding different types of intelligence collection

Different Types of Intelligence Collection



Reference: https://robindimyan.medium.com/geopolitical-cyber-risk-going-beyond-the-industry-and-region-3581465c7e3f

Strategic vs. Tactical Collection

A target may be capable of:

- Supplying information that supports long-term policies.
- Fulfilling several intelligence requirements simultaneously.
- Offering information that an agency consistently requires.

Targeting is expected to be persistent, adaptive and long term, but unlikely to employ advanced, event-based capabilities.

STRATEGIC COLLECTION

A target may be capable of:

- Fulfilling intelligence needs that are *immediate* and *critical*.
- Providing information that an agency is unable to obtain through alternative sources.

Targeting is expected to be persistent and adaptive, and more likely to employ advanced, event-based capabilities.

TACTICAL COLLECTION

Beginning

STEP 1

Consider your business and see if there is anything about you that may concern political, economic or military interests of any country

STEP 2

Try to identify the countries whose interests may lead their intelligence services to target you. Try to get more specific about why they might target you

STEP 3

For each country, try to understand what kind of collection effort you’re more likely to be a target of; strategic, tactical, or both

STEP 4

Map all these information with the cyber capabilities of each country

End

China's Foreign Investments

July 17, 2018

In May, a minister in the government of President Recep Tayyip Erdogan said the country is in talks with Alibaba and Amazon.com over possible investments in Turkey. A venture capital source said Amazon is expected to begin operating in Turkey later this year. Alibaba's investment in Trendyol was likely an effort by the Chinese company to get a jump on its U.S. rival.

1 Dec, 2021

China will prioritize quality over quantity in growing e-commerce as the sector matures and devises new indexes for its development to enable it to play a notable role in catalyzing high-quality growth during the 14th Five-Year Plan period (2021-25), experts and industrial insiders said.

01.12.2021

Aug 15, 2018

Alibaba flexes its muscles on its commitment to its international expansion plans.

China's e-commerce major Alibaba Group has paid $750m to become a major shareholder of Turkish e-commerce startup Trendyol, according to an account by *Axios*. The Turkish fashion sales firm counts the likes of Tiger Global, Kleiner Perkins, and Earlybird Venture Capital as backers.

Key Takeaways

- Nation-state cyber intrusions typically fall into three categories: denial (military), coercion (diplomatic), and espionage.

- The motives behind cyber espionage are shaped by a nation's political, economic, and military objectives.

- Businesses may be targeted by intelligence agencies if they hold assets related to these objectives, such as products, information, employees, customers, or access.

Questions?

robindimyan.medium.com