Predictive Cyber Defense

Early Warning Intelligence & Forecasting

Whoami?

Red Team Lead @ HelloFresh

Creator @ predictivedefense.io

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
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.

Reactive vs. Proactive vs. Predictive Defense

Reactive Defense:

- “There’s an ongoing campaign and here are the IOC’s. Let’s hunt for these in our network and feed this info to our prevention systems.” (Tactical decision making)

Proactive Defense:

- “There’s an actor known to target our industry and here are the TTPs they’re likely to use. Let’s build detections around these and prioritise the patching of ABC vulnerabilities.” (Tactical decision making)

Predictive Defense:

- “There’s a high probability of an XYZ attack occurring in the following [time] period. Let’s formulate a preparation plan to lessen its impact and enhance our response.” (Tactical decision making)

Reactive vs. Proactive vs. Predictive Defense

Reactive Defense:

- “We've faced numerous DDoS attacks causing downtime this year. Let's invest in a DDoS protection solution.” (Strategic decision making)

Proactive Defense:

- “Based on our attack surface and threat models, exposed secrets are one the most impactful threats we could face. Let's plan to implement a secret management solution.” (Strategic decision making)

Predictive Defense:

- “We expect that cybercriminals will shift from credential stuffing to cookie/session-based attacks in the coming years due to X, Y, and Z reasons. Let's initiate a plan to address session management issues in our systems next year.” (Strategic decision making)

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?

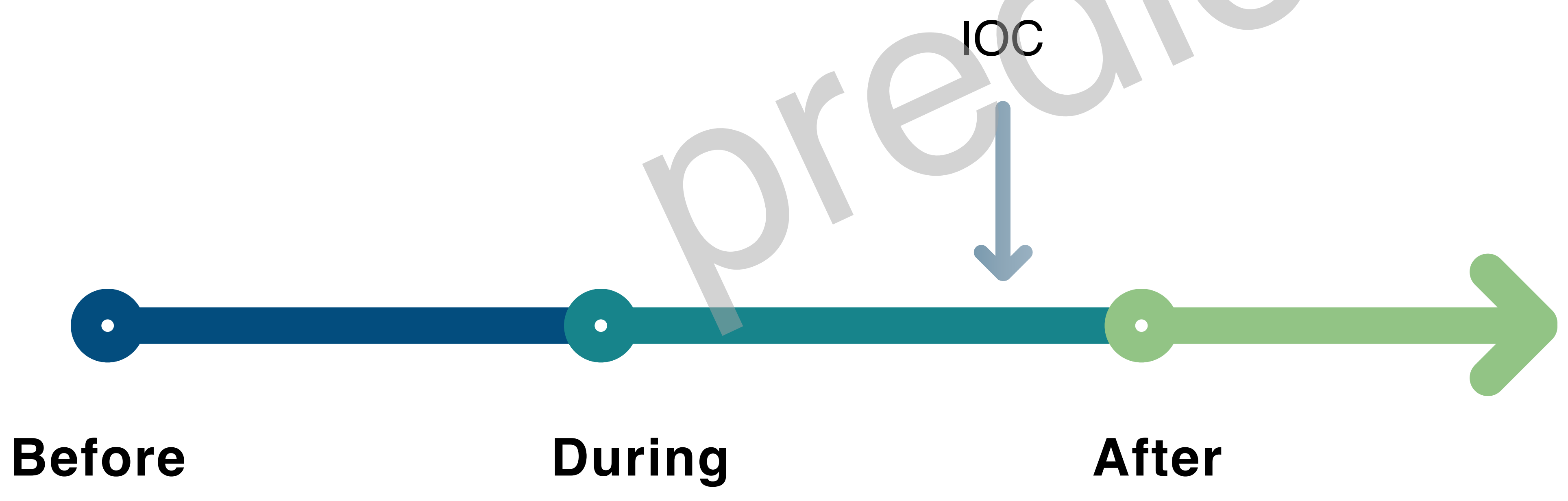
EARLY WARNING SYSTEM

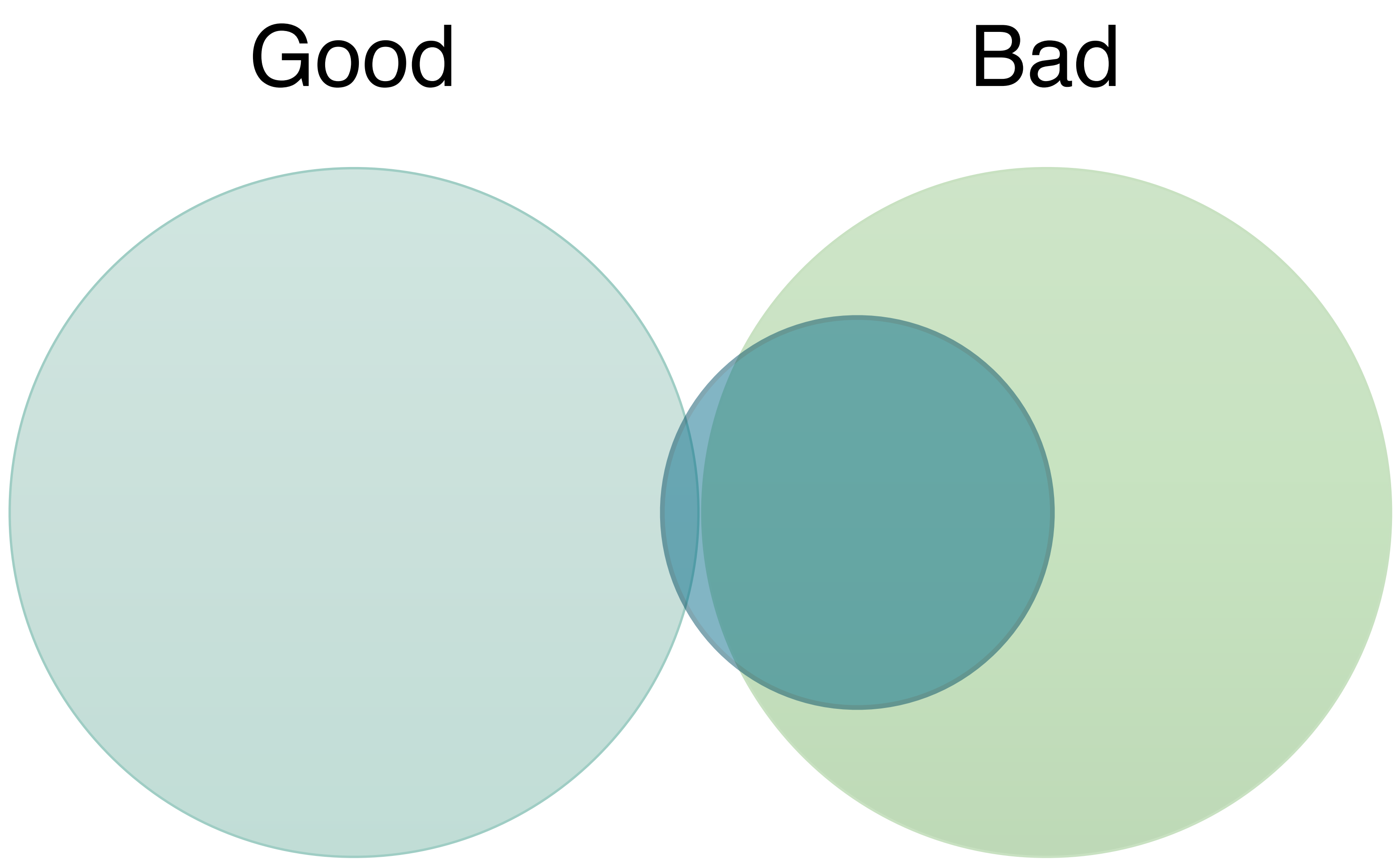
Introduction to Predictive Defense

Comparing intelligence products

Indicators of Compromise, signatures:

- These include known malicious IPs, hostnames, and files
- The strategy is to prevent the execution of malicious activities
- This approach is highly accurate but may miss some threats (**high** precision, **low** recall)

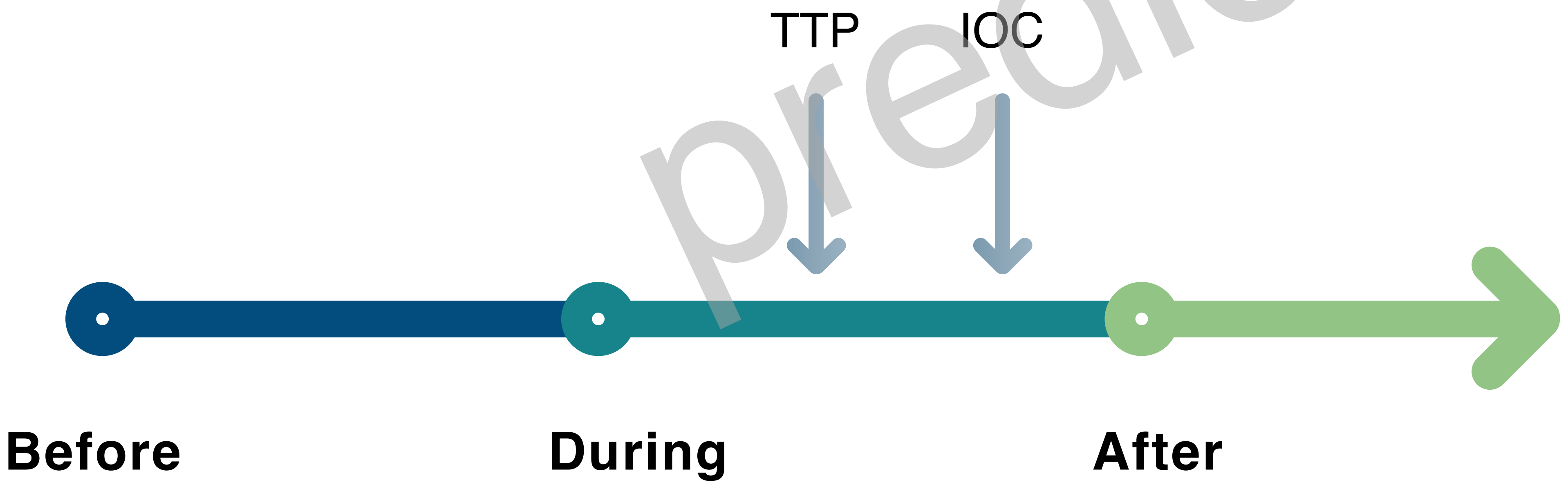


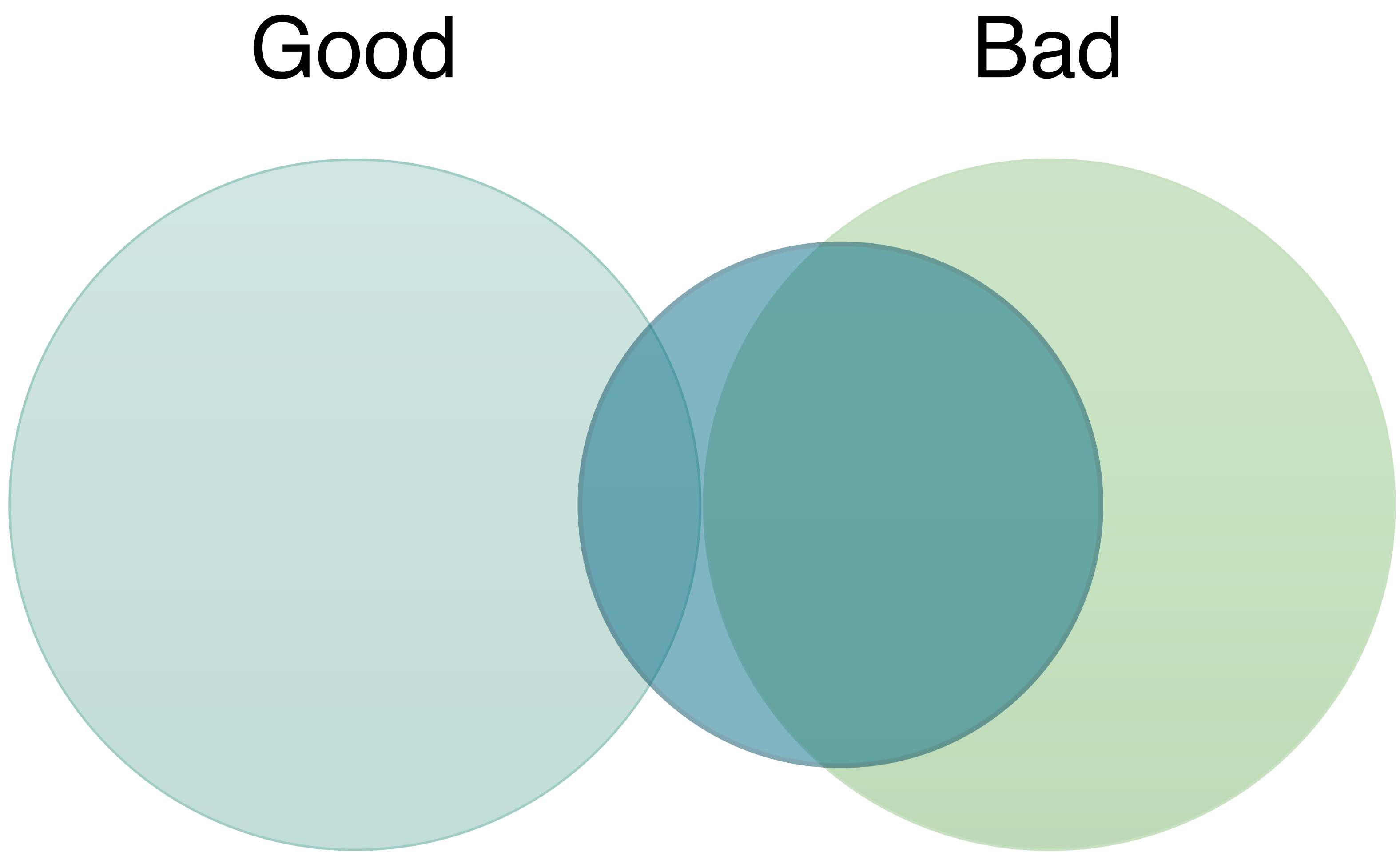


Comparing intelligence products

Indicators of Attack, TTPs:

- Focuses on behavioural indicators associated with known malicious activities
- The strategy is to quickly detect harmful activities so that there can be a timely response
- This method is more flexible than using signatures, though it may lead to more false positives
- It offers moderate accuracy and detection rate (**medium** precision, **medium** recall)



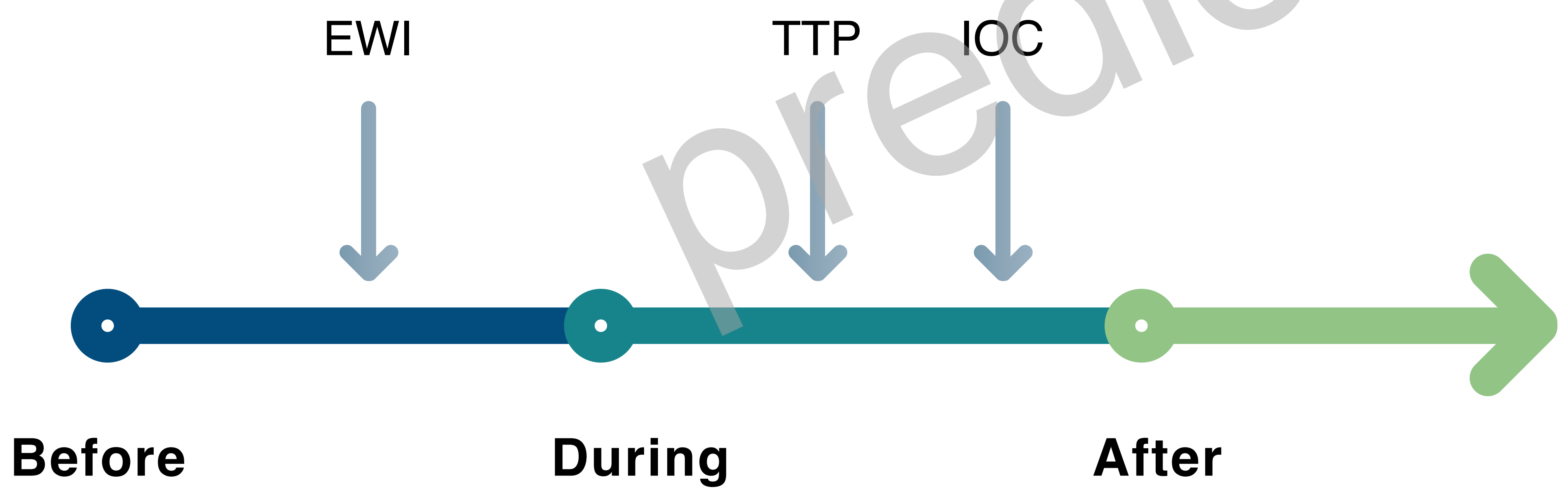


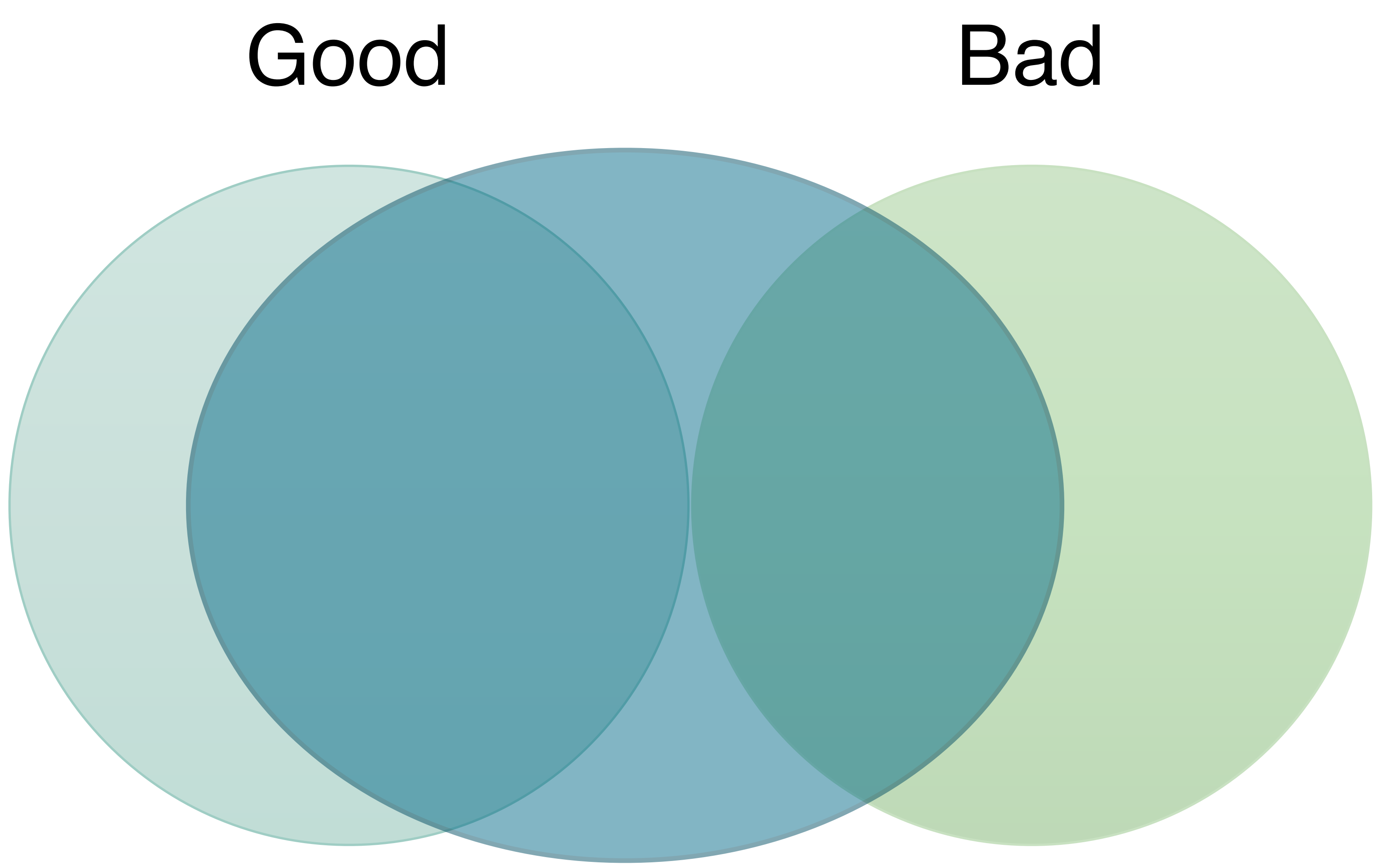
Comparing intelligence products

Early Warnings:

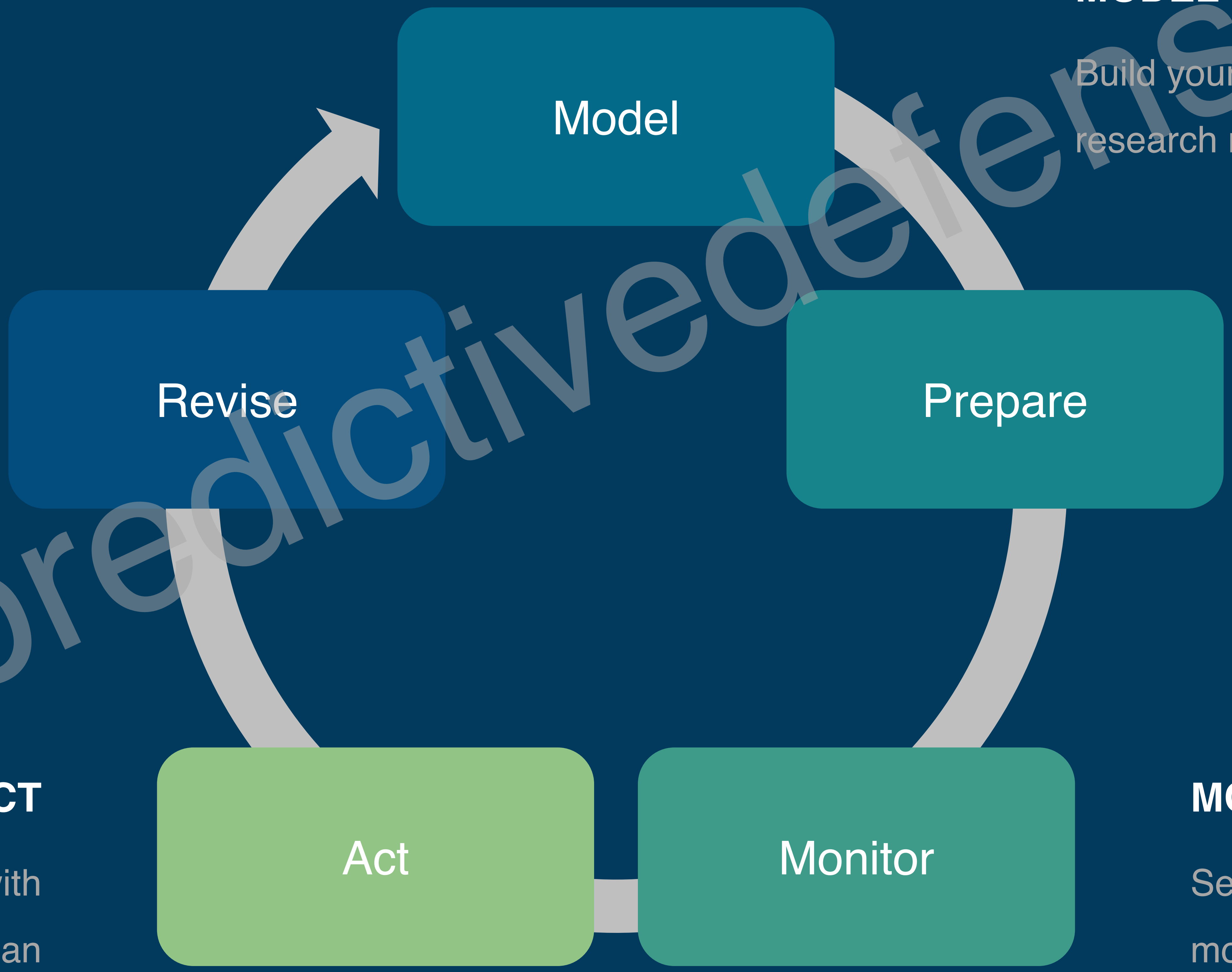
- Involves monitoring precursor events that could lead to malicious activities
- The strategy is to identify a potential malicious event during its development stage
- While this method captures a wide range of activities, it is less precise (**low** precision, **medium** recall)

Trading off precision in order to gain extra response time.





Predictive Defense



MODEL

Build your predictive model using the research methodologies

PREPARE

Devise your response plan to act on certain probabilities of an attack

MONITOR

Set up the systems and start monitoring for the early warnings

ACT

Act on early warnings accordingly with the pre-determined plan

REVISE

Revisit your predictive model and response plans whenever needed

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.

Research Approaches

3. Hypothesis-driven research

- You make a hypothesis about how a certain type of attack may unfold.
- Then, you collect data from different sources and analyse to confirm or refute your hypothesis.

4. Probabilistic attack trees

- You create an attack tree to model your environment and assign probabilities of success for each step.
- Then, you choose one step as an indicator and estimate the number of attempts required to accomplish the attacker's goal.

Infostealer Infections

Infostealer Infections

What does a typical malspam look like?

- Set up your C2 and other infrastructure
- Build the malware strain of your choice (Redline, Vidar, Raccoon)
- Build a dropper (optional)
- Set up your distribution infrastructure
    - Malspam -> Email server, malware host
    - Malvertising -> Landing page, advertising platforms
    - Torrent-like websites -> Application to trojanize, websites for distribution

What could be some early signs for this type of attack?

Infostealer Infections

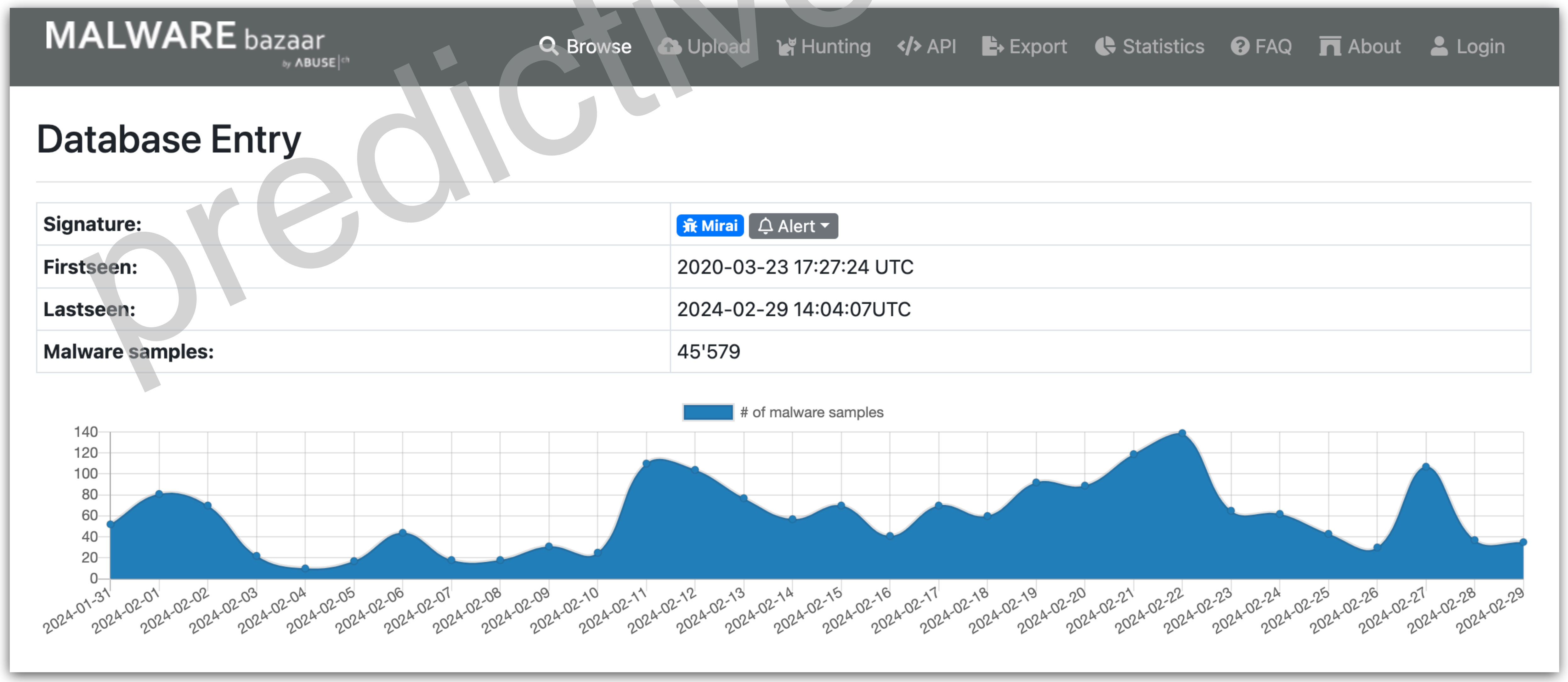
Our hypothesis:

- Malspam is an indiscriminate attack
- While profiling these intrusions is hard, it is reasonable to assume they will occur in "waves"
- If only there were a website where we could monitor these surges...

Infostealer Infections

Our hypothesis:

- Malspam is an indiscriminate attack
- While profiling these intrusions is hard, it is reasonable to assume they will occur in "waves"
- If only there were a website where we could monitor these surges...

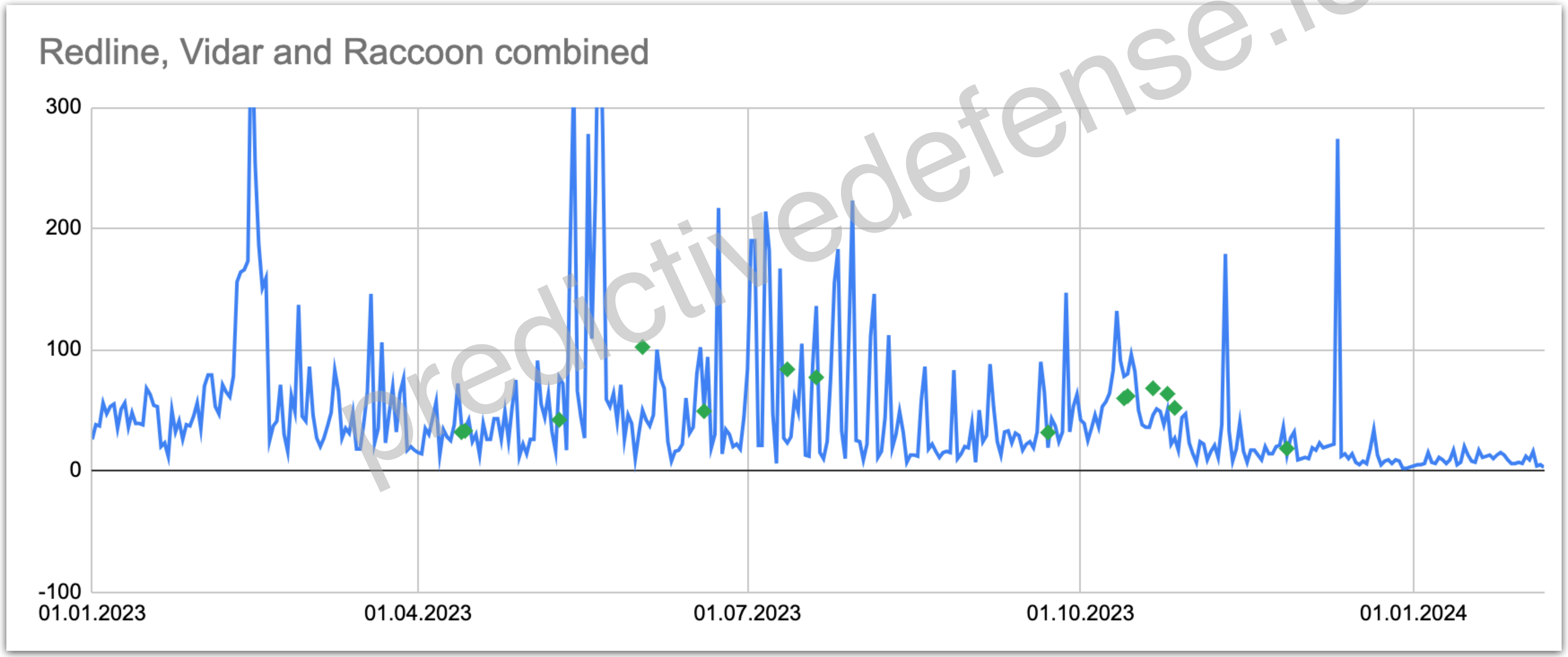


Database Entry

Signature:	Mirai Alert
Firstseen:	2020-03-23 17:27:24 UTC
Lastseen:	2024-02-29 14:04:07UTC
Malware samples:	45'579

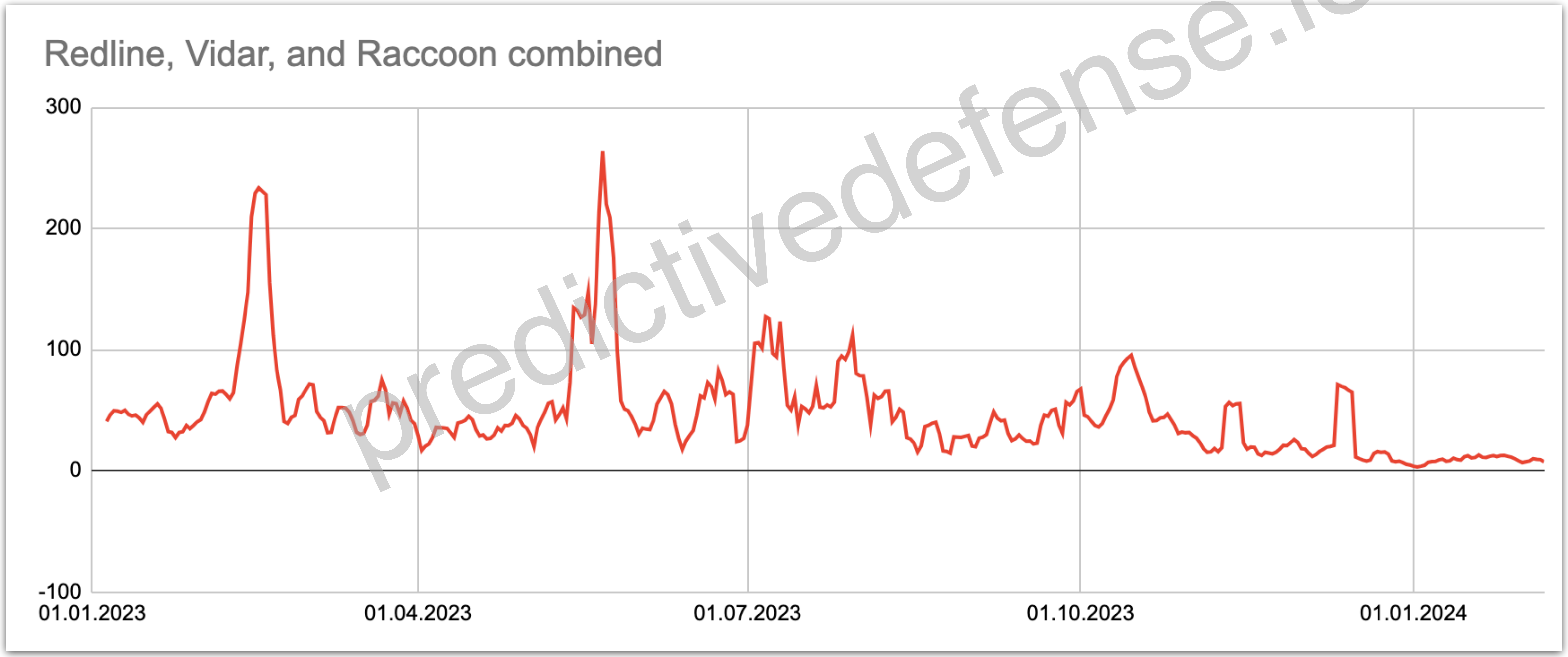
Infostealer Infections

Collection is easy. Modelling is hard...



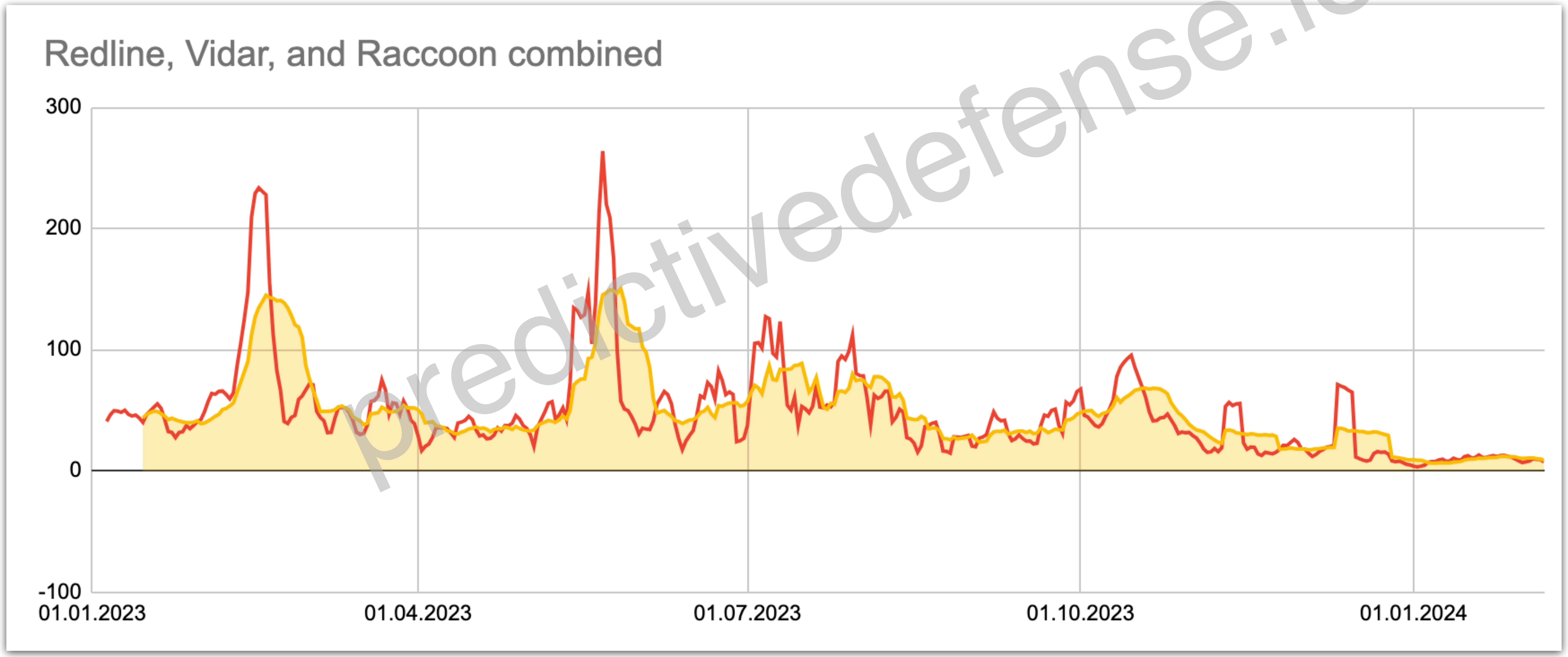
Infostealer Infections

Simple moving average (5 days)



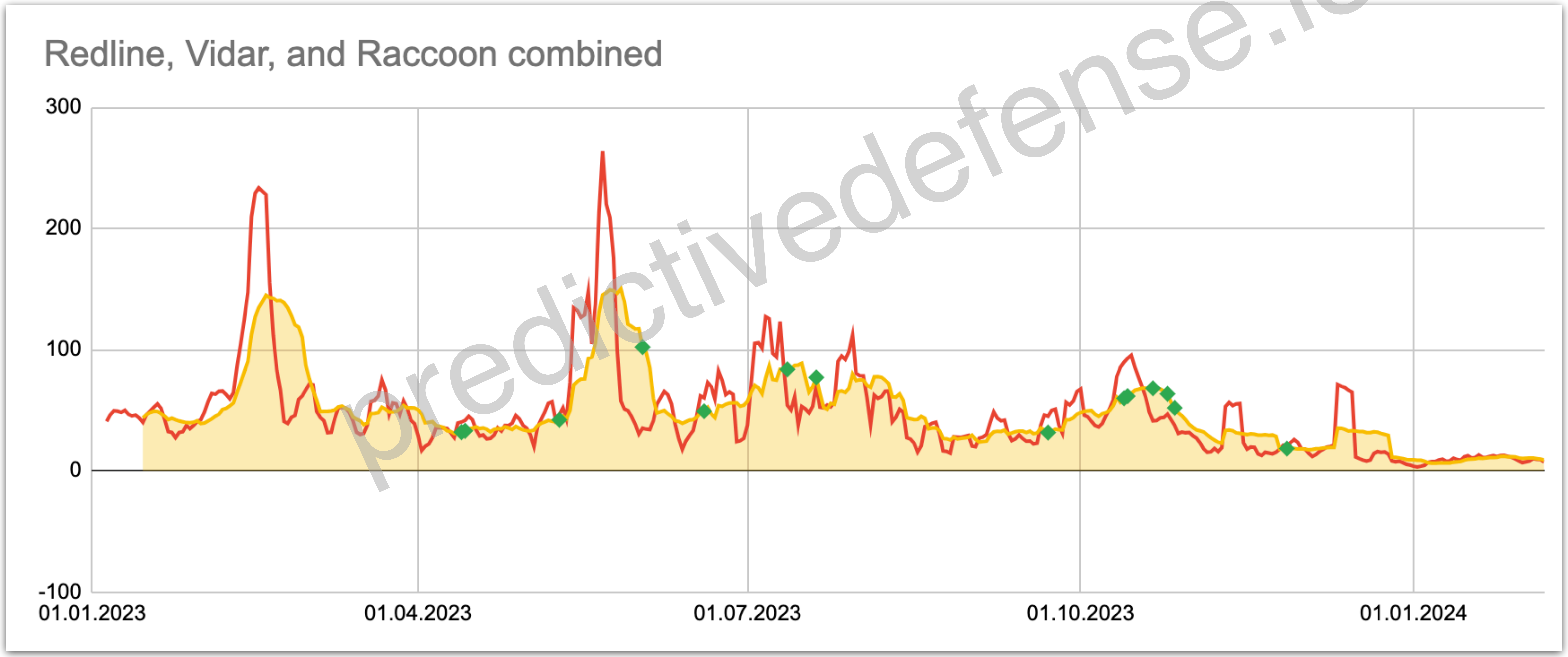
Infostealer Infections

SMA(5 days) vs. SMA(15 days)



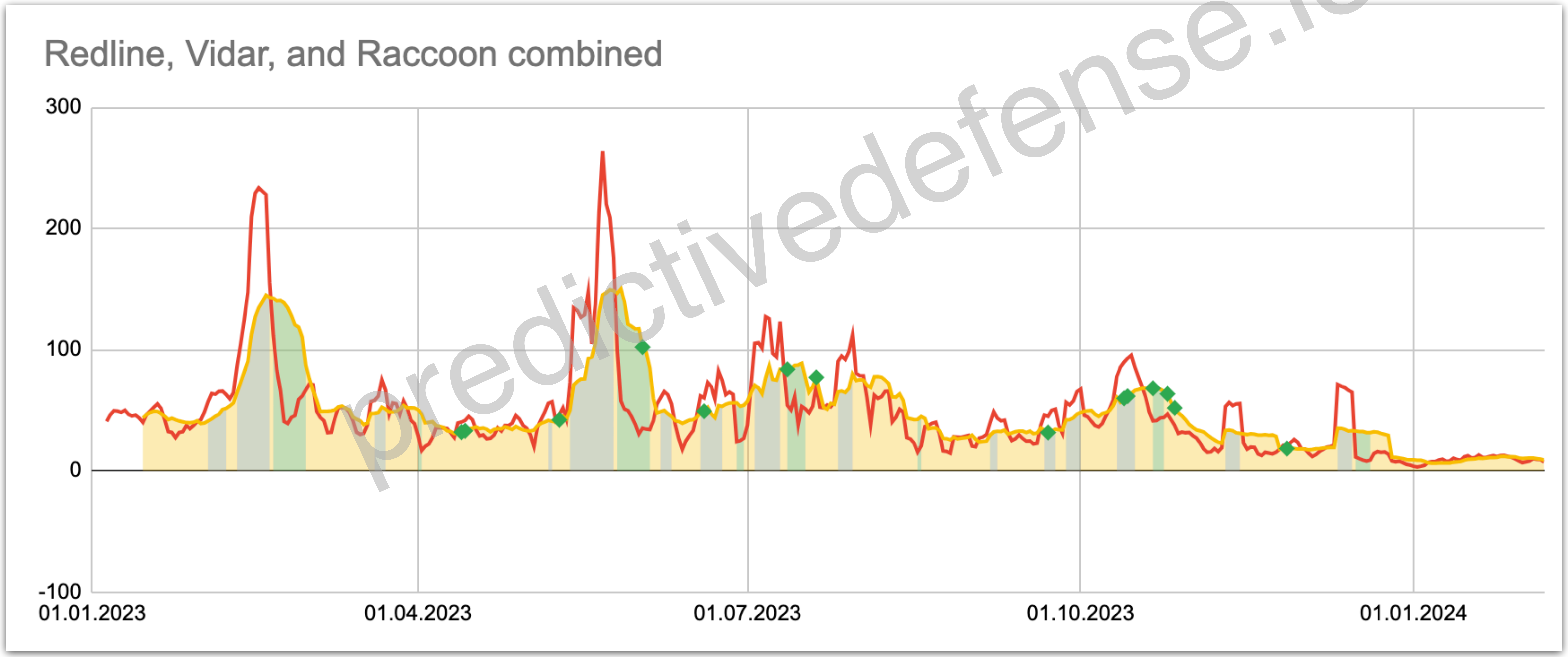
Infostealer Infections

SMA(5 days) vs. SMA(15 days)



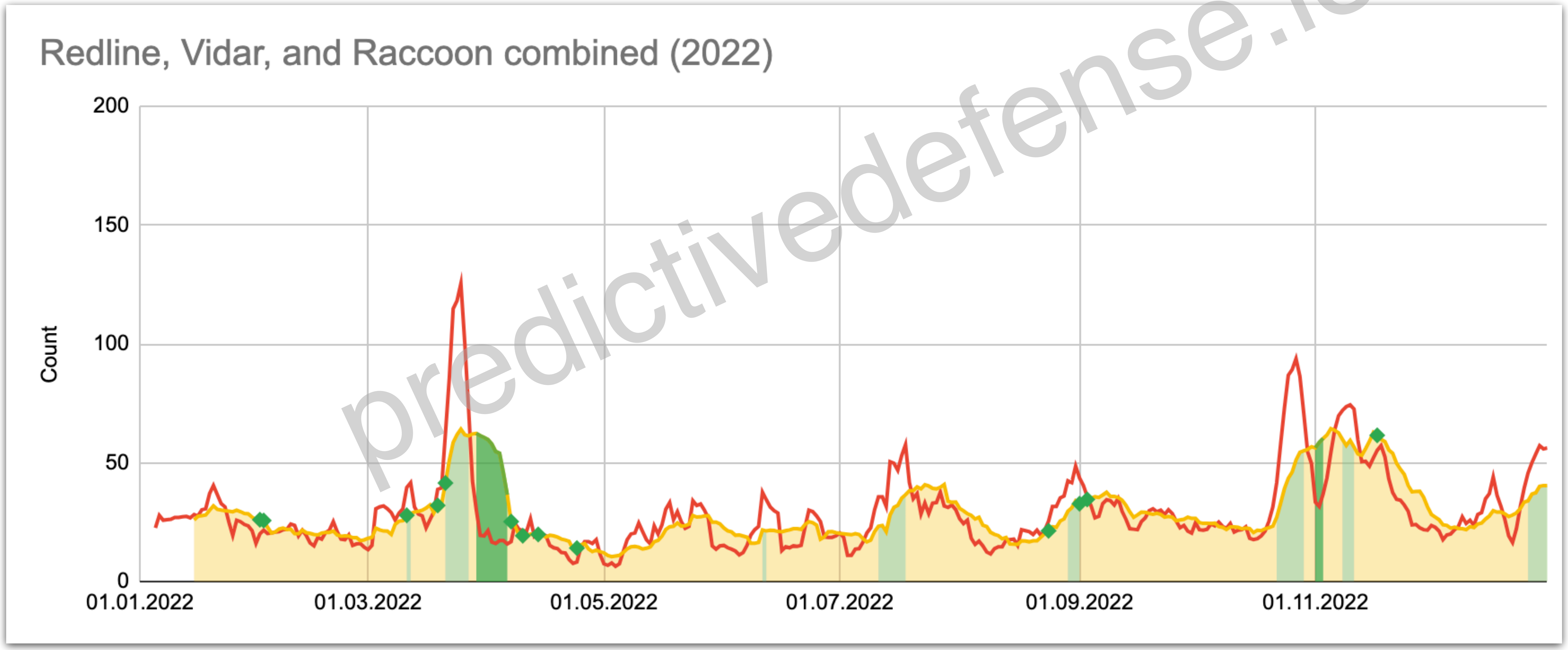
Infostealer Infections

Model: **SMA(5 days) - SMA(15 days) > 10** **OR** **SMA(5 days) - SMA(15 days) < -20**



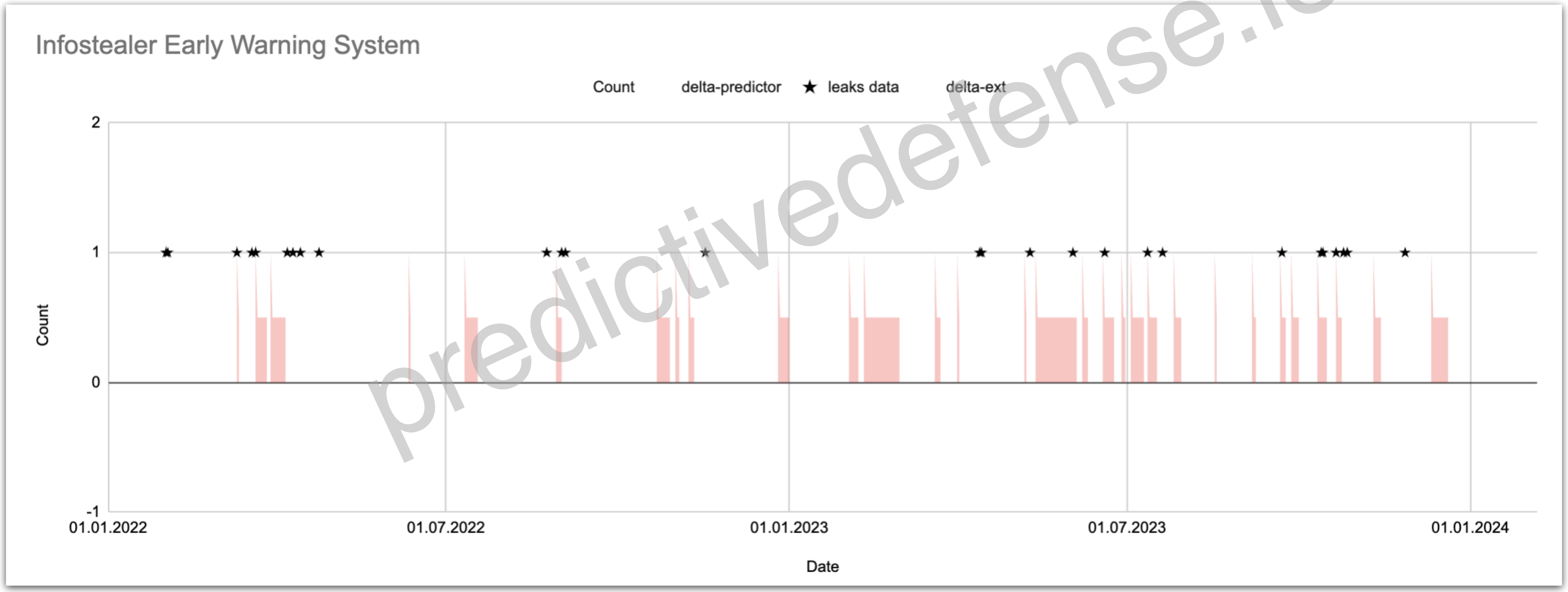
Infostealer Infections

Always validate your model!



Infostealer Infections

Period: 2 years, Total alerts: 30, Precision: 40%, Recall: 88%



Infostealer Infections

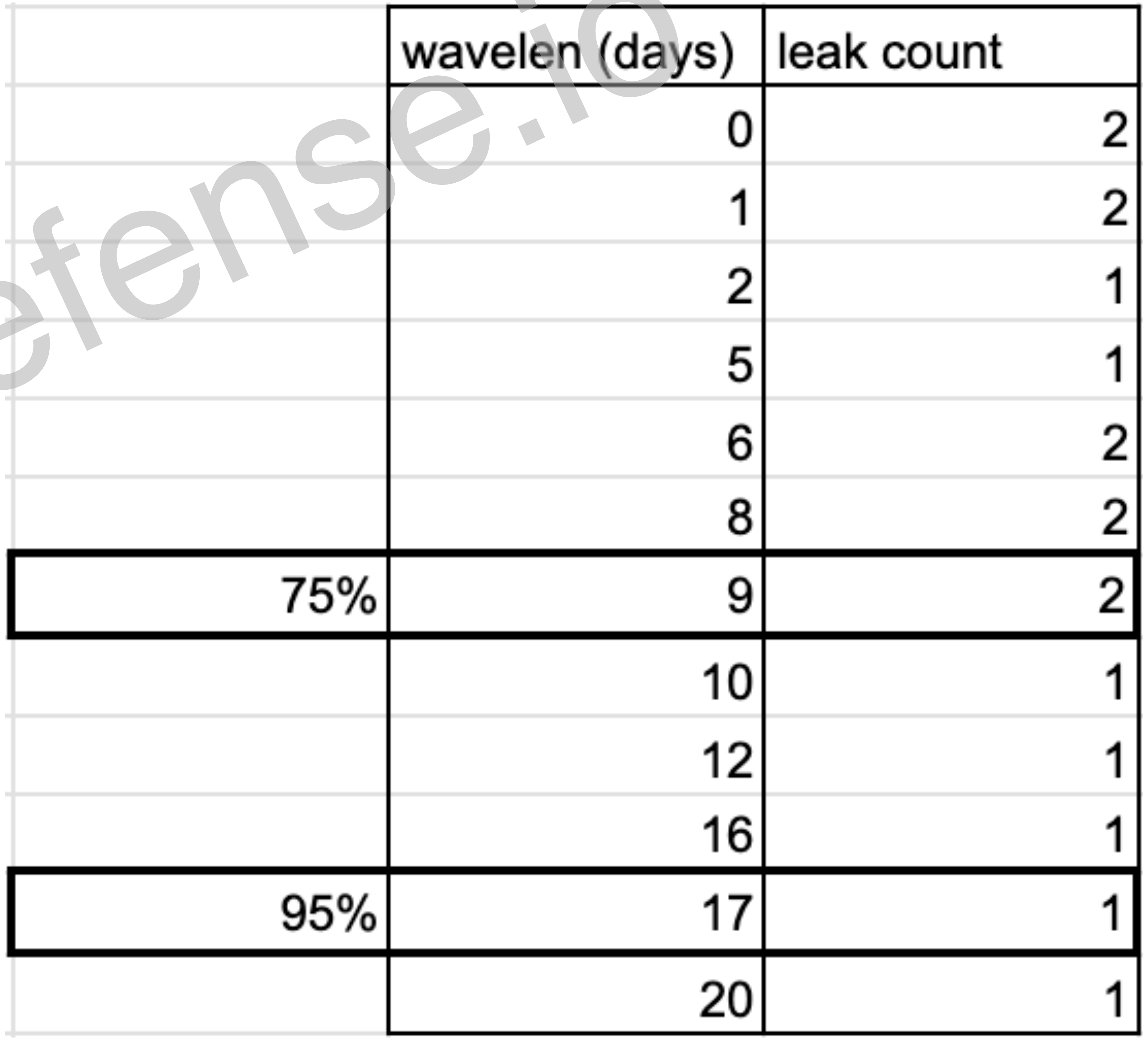
Calculating signal lifetime:

- 75% of the infections occurred within the first nine days following a warning's generation
- 20% took place between the 9th and 17th days

Warning 1-9 days = **HIGH** RISK

10-17 days = **MEDIUM** RISK

> 18 days = **LOW** RISK



	wavelen (days)	leak count
	0	2
	1	2
	2	1
	5	1
	6	2
	8	2
75%	9	2
	10	1
	12	1
	16	1
95%	17	1
	20	1

Proactive Incident Response

Proactive Countermeasure Plan: Infostealer Infections (Employee credential leak)

THREAT LEVEL	DEFINITION	MEASURES
HIGH	Warning issued due to a recent surge in submitted samples of infostealer malware (75% probability of infection)	1. Issue a company-wide message to raise awareness about the heightened threat of malware 2. Force a targeted password reset on X% of employees upon weak signs of compromise 3. Enable more restrictive conditional access policies for high-privileged accounts
MEDIUM	10 days have passed since the initial warning (20% probability of infection)	Assume breach and initiate a threat hunt focusing on regions and employees with higher exposure
LOW	18 days have passed since the initial warning (5% probability of infection)	Follow-up communication is sent to the employees to inform them

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?

Profiling Leery Turtle Attacks

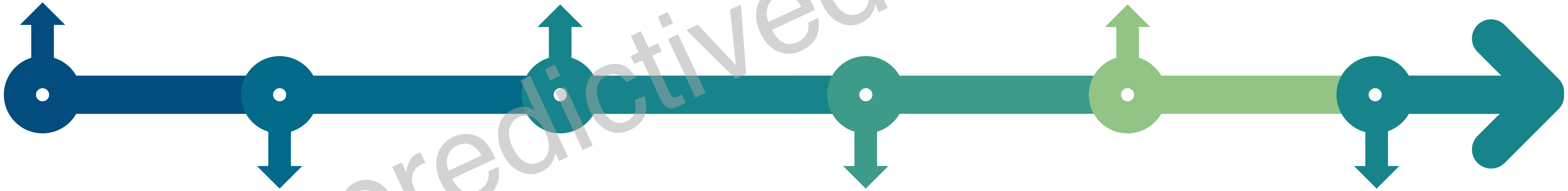
Spear-phishing campaigns targeting crypto-exchange businesses worldwide that are later attributed to North Korea.

- 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.

New infrastructure

Scan the internet to spot new infrastructure based on the profiles

Infrastructure pivoting

New domains fitting the pattern
New servers with similar config

New malware samples

Monitor malware families that are of interest using open sources

Vendor reports / OSINT

Recent reports of the same campaign that are of interest

Campaign start

Building the Early Warning System

Data analysis!

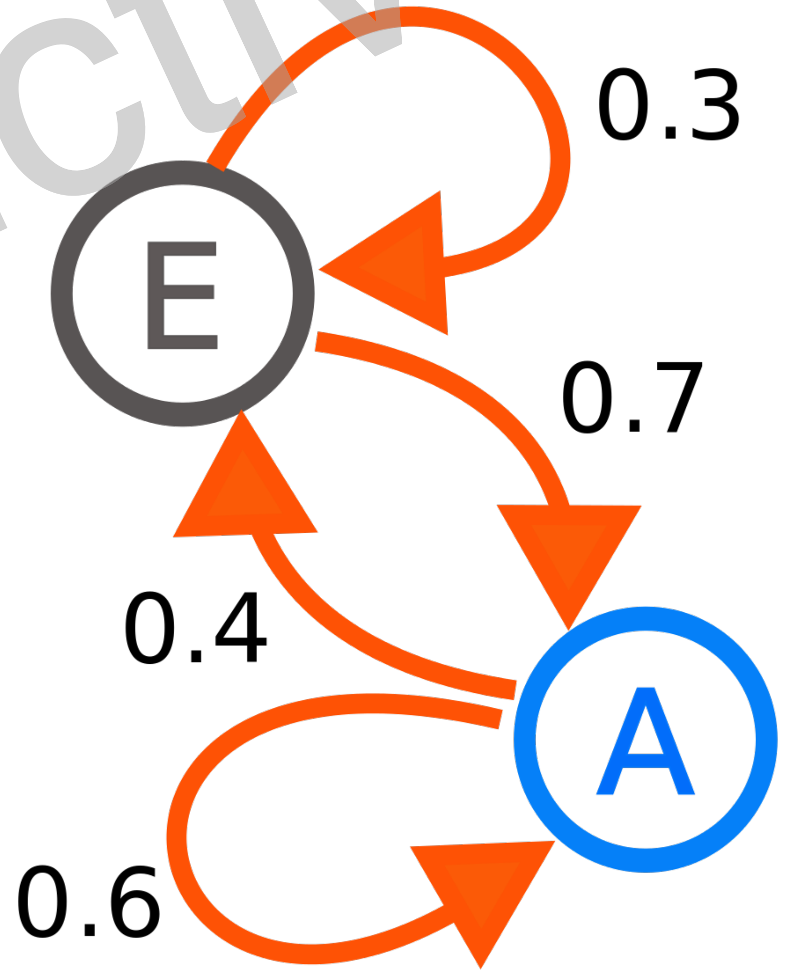
- Extract a history of these signals retrospectively (if possible)
- Compare with the history of spear-phishing attacks you have received
- Try different weights and combinations to see which model makes the best prediction
- You can use mean-time between two attacks as the signal lifetime
  - You can 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

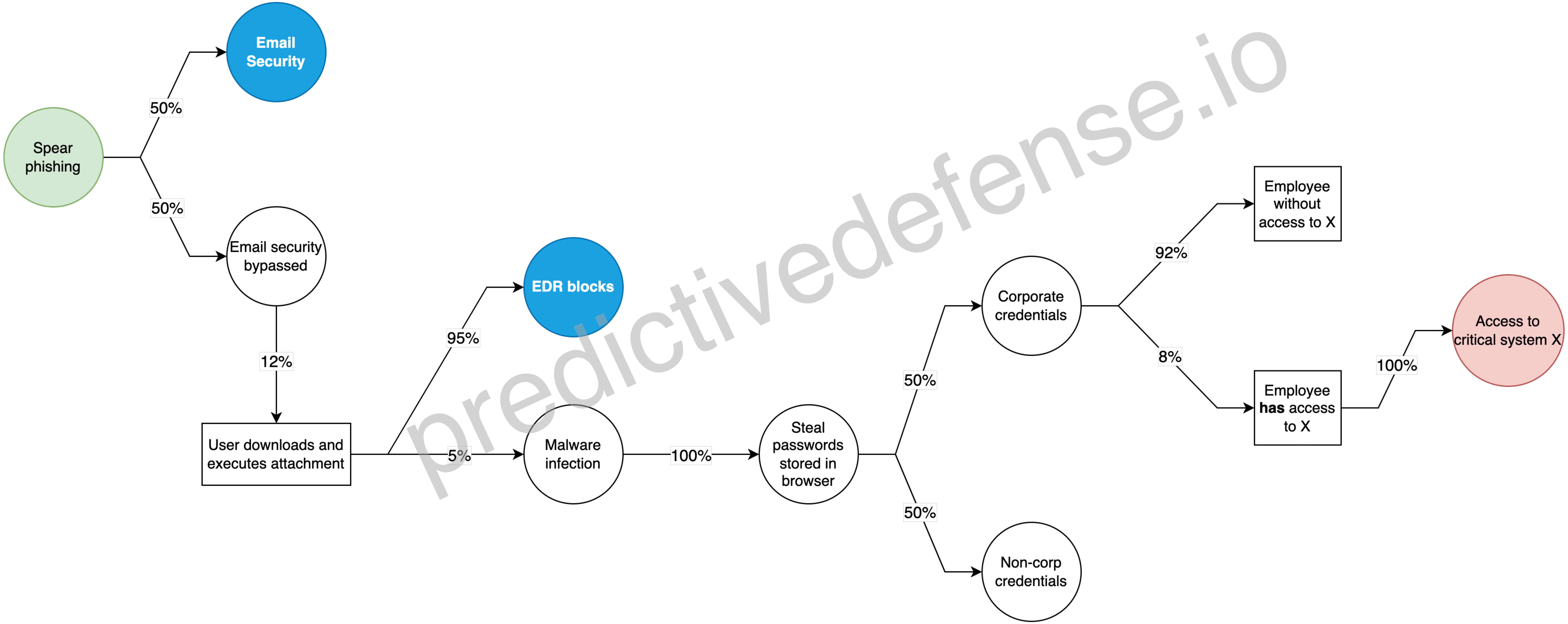
Spear-Phishing - Reloaded

Markov Chains

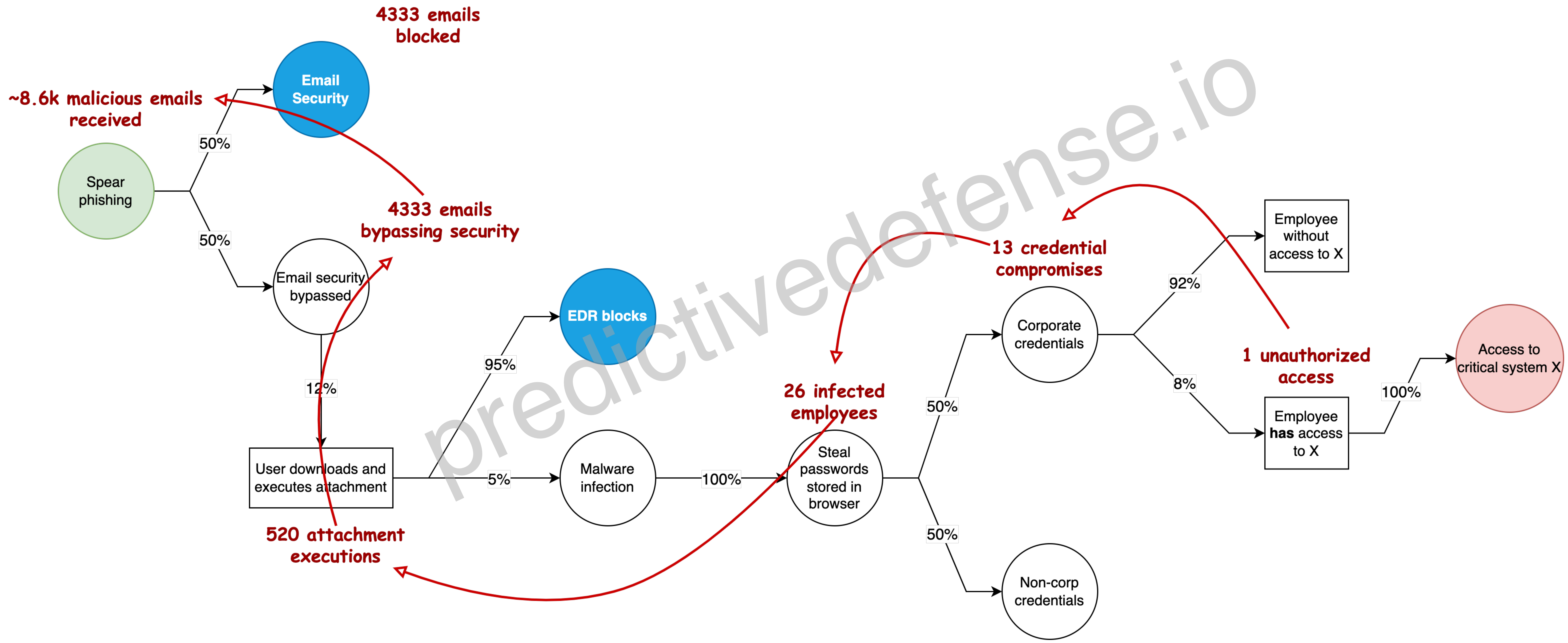
A **Markov chain** or **Markov process** is a stochastic model describing a sequence of possible events in which the probability of each event depends only on the state attained in the previous event. Informally, this may be thought of as, "What happens next depends only on the state of affairs now." (Wikipedia)



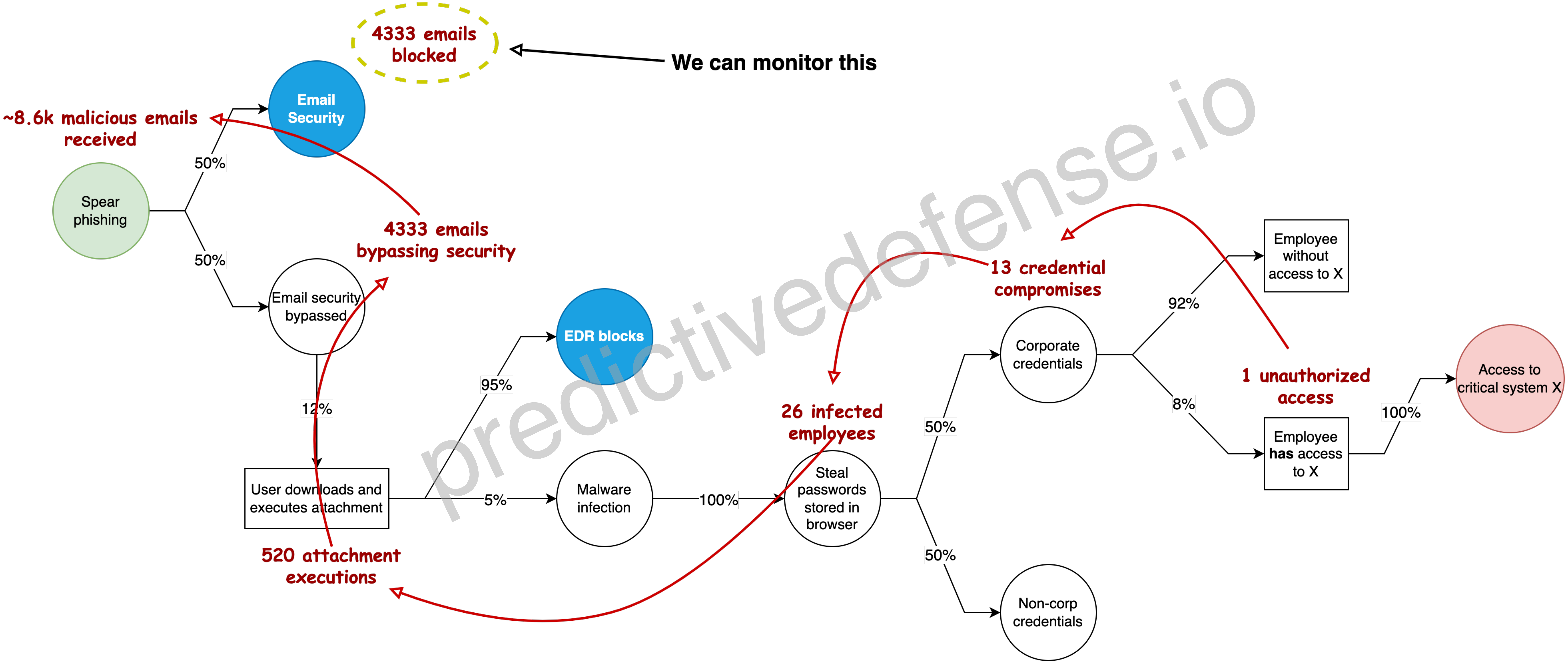
Probabilistic Attack Tree


Spear phishing
50%
Email Security
50%
Email security bypassed
12%
User downloads and executes attachment
95%
EDR blocks
5%
Malware infection
100%
Steal passwords stored in browser
50%
Corporate credentials
50%
Non-corp credentials
92%
Employee without access to X
8%
Employee **has** access to X
100%
Access to critical system X

Probabilistic Attack Tree


4333 emails blocked
~8.6k malicious emails received
Email Security
50%
Spear phishing
50%
4333 emails bypassing security
Email security bypassed
12%
EDR blocks
95%
User downloads and executes attachment
5%
Malware infection
100%
520 attachment executions
26 infected employees
Steal passwords stored in browser
13 credential compromises
50%
Corporate credentials
50%
Non-corp credentials
92%
Employee without access to X
8%
Employee has access to X
1 unauthorized access
100%
Access to critical system X

Probabilistic Attack Tree


4333 emails blocked
We can monitor this
~8.6k malicious emails received
Email Security
50%
Spear phishing
50%
4333 emails bypassing security
Email security bypassed
12%
EDR blocks
95%
User downloads and executes attachment
5%
Malware infection
100%
520 attachment executions
26 infected employees
Steal passwords stored in browser
50%
50%
13 credential compromises
Corporate credentials
Non-corp credentials
92%
8%
Employee without access to X
Employee **has** access to X
1 unauthorized access
100%
Access to critical system X

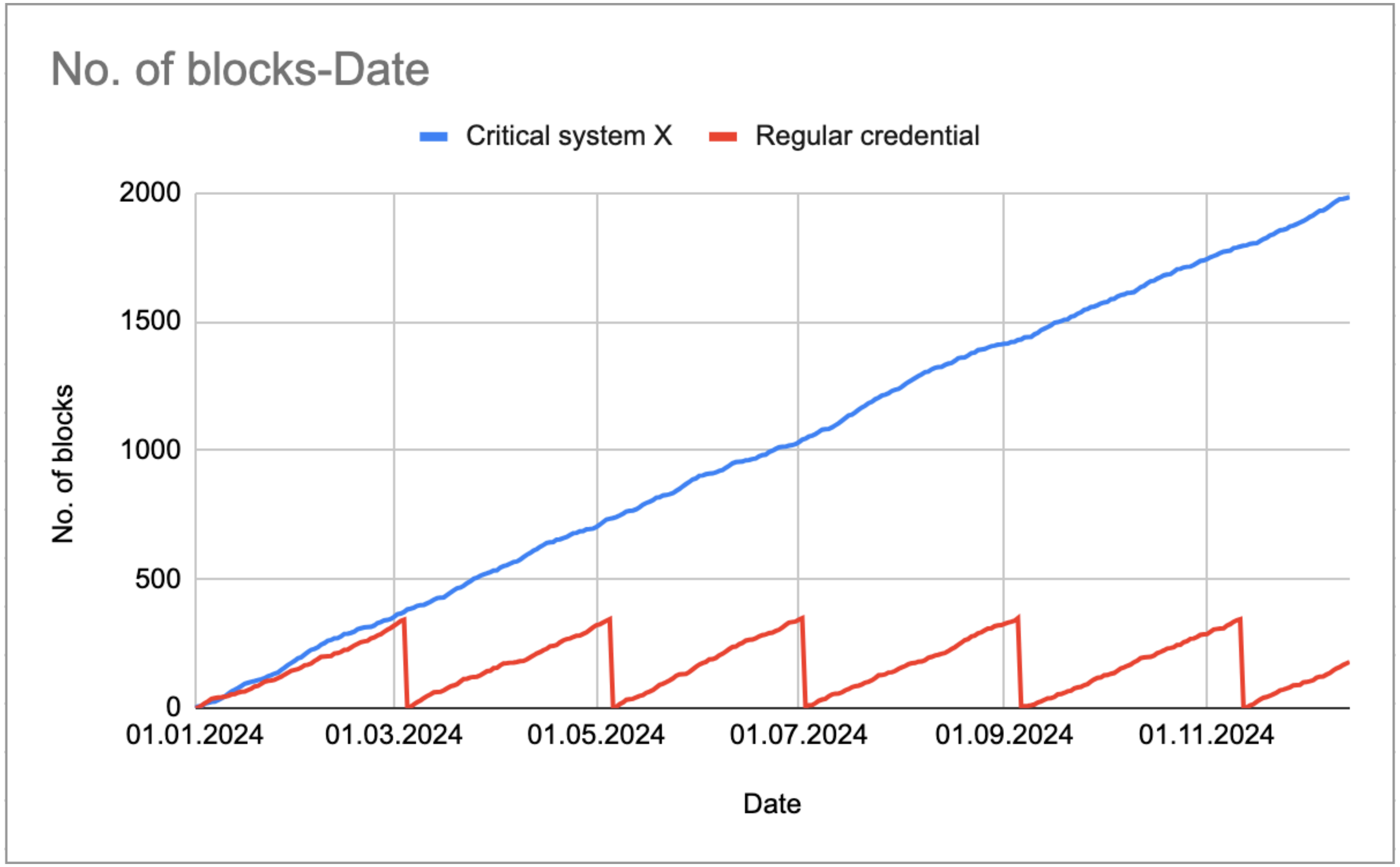
Building the Early Warning System

Our assumptions:

- If more than **4,300 emails** with malicious attachments are blocked within a certain period, there is **high** likelihood of a compromise of credentials for critical system X.
- If more than **350 emails** with malicious attachments are blocked within a certain period, there is a high likelihood of *regular* corporate credential compromise.

Building the Early Warning System

Rate: 1 to 10 malicious emails daily



I&W Analysis

Email security gateway

Monitor email security alerts for number of phishings containing malicious attachment

Employee account breach

When number of blocks exceed 350, start threat hunting for compromised employees

Critical system breach

When number of blocks exceed 4300, start reviewing access logs for critical system X

Proactive Incident Response

Proactive Countermeasure Plan: Spear-phishing Attack		
THREAT LEVEL	**DEFINITION**	**MEASURES**
LEVEL 0	The time period amounting to "mean-time between two attacks" has passed without any detected spear-phishings	Assume breach and initiate a threat hunt focusing on regions and employees with higher exposure
LEVEL 1	A warning has been generated with **<70%** probability	1. Issue a company-wide message to raise awareness about the heightened threat of spear-phishing 2. Force a targeted password reset on X% of employees upon weak signals of compromise 3. Temporarily enable more sensitive TA0002 (Execution) detection rules to enhance monitoring
LEVEL 2	A warning has been generated with **>70%** probability.	1. Enable more restrictive conditional access policies for high-privileged accounts 2. Temporarily block TA0002 (Execution) techniques by group policies
LEVEL 3	A warning has been generated with **>90%** probability	1. Reimage the devices of employees who have access to critical systems and rotate their passwords 2. Users at higher risk of compromise are temporarily revoked some of their access

Credential Stuffing

Collecting Data

Intelligence platforms

Open source intelligence

Azure logs

Darkweb mentions

Infostealer leaked creds

Coupon code sales

Reported phishing emails

DDoS attacks

Web exploit attempts

Azure risky sign-ins

SIEM events

Web Application Firewall

Internal reports

Credential Stuffing Attacks

What does a typical credential stuffing attack look like?

- Curate a username:password combolist
- Test the defenses of your target organization (rate limits, bot protection etc.)
- Gather a live proxies list
- Launch your attack over several days and by constantly switching proxies
- Sell the compromised accounts in cybercrime mediums

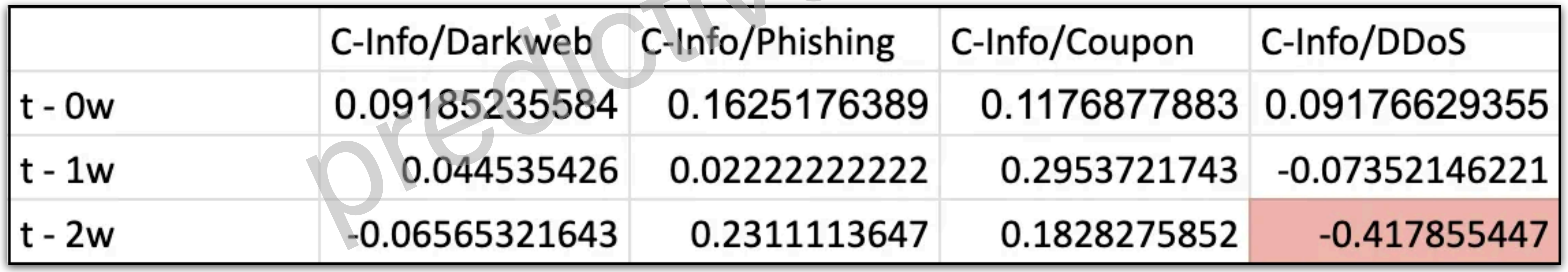
What could be some early signs for this type of attack?

Credential Stuffing Attacks

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.

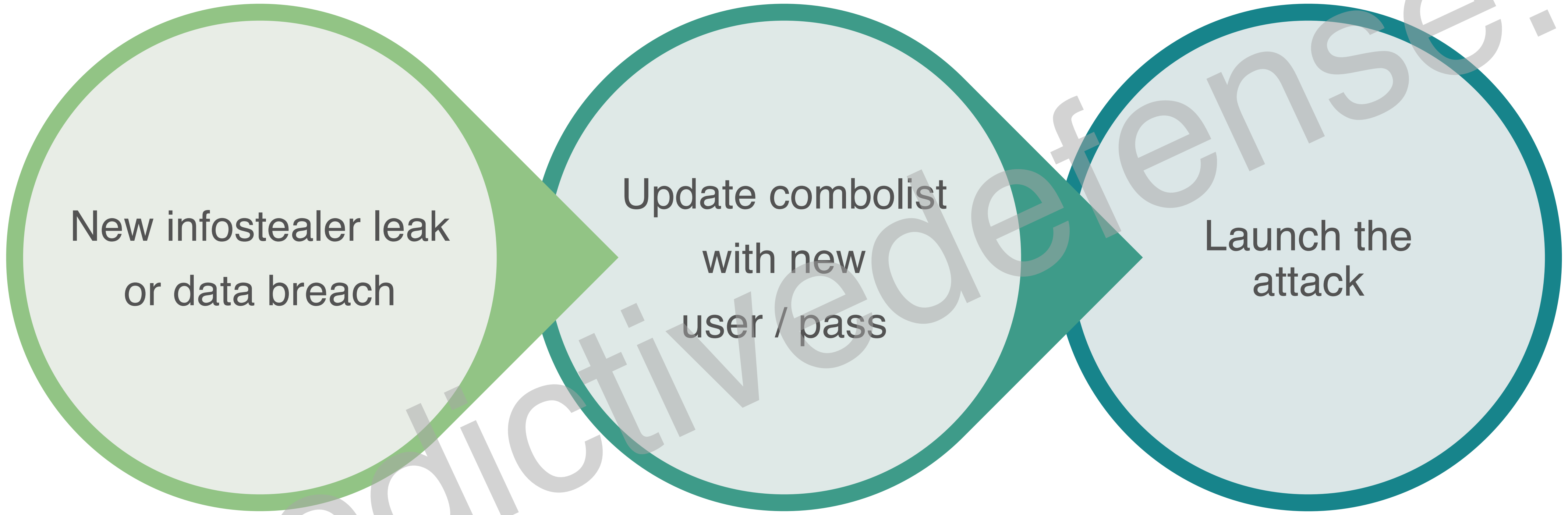
Afterward, the binary combinations of these events are compared using a correlation function.



	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

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

Constructing the Hypothesis


New infostealer leak or data breach
Update combolist with new user / pass
Launch the attack

If accounts belonging to our organization have been leaked in publicly shared Infostealer logs, 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 leaked accounts

Detect leaked accounts belonging to our organization

Alerting

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

Proactive Incident Response

Proactive Countermeasure Plan: Credential Stuffing Attack

THREAT LEVEL	DEFINITION	MEASURES
ELEVATED	Recent data breaches and infostealer logs have been found to contain credentials belonging to our customers	1. Issue a message to devops/monitoring teams about the heightened threat of credential stuffing 2. Temporarily tighten the WAF rules and rate limits
NORMAL	14 days have been passed since the initial warning	No actions

Mass Exploitation

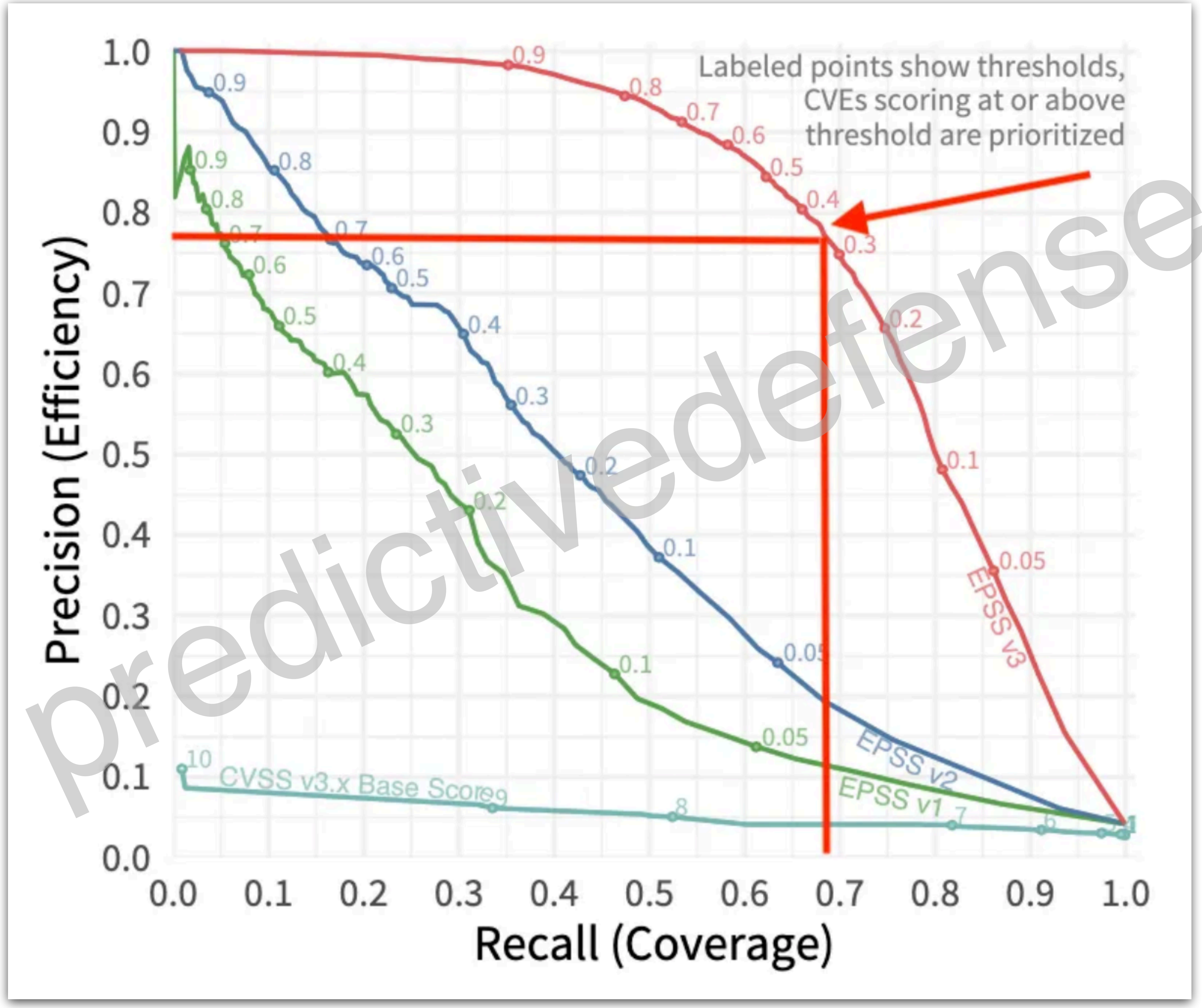
Mass Exploitation

Exploit Prediction Scoring System (EPSS)

EPSS provides a probability estimate of a vulnerability being exploited within 30 days of its disclosure.

- https://www.first.org/epss/model
- https://stephenshaffer.io/determining-epss-score-thresholds-for-prioritization-86e08db21798

Mass Exploitation

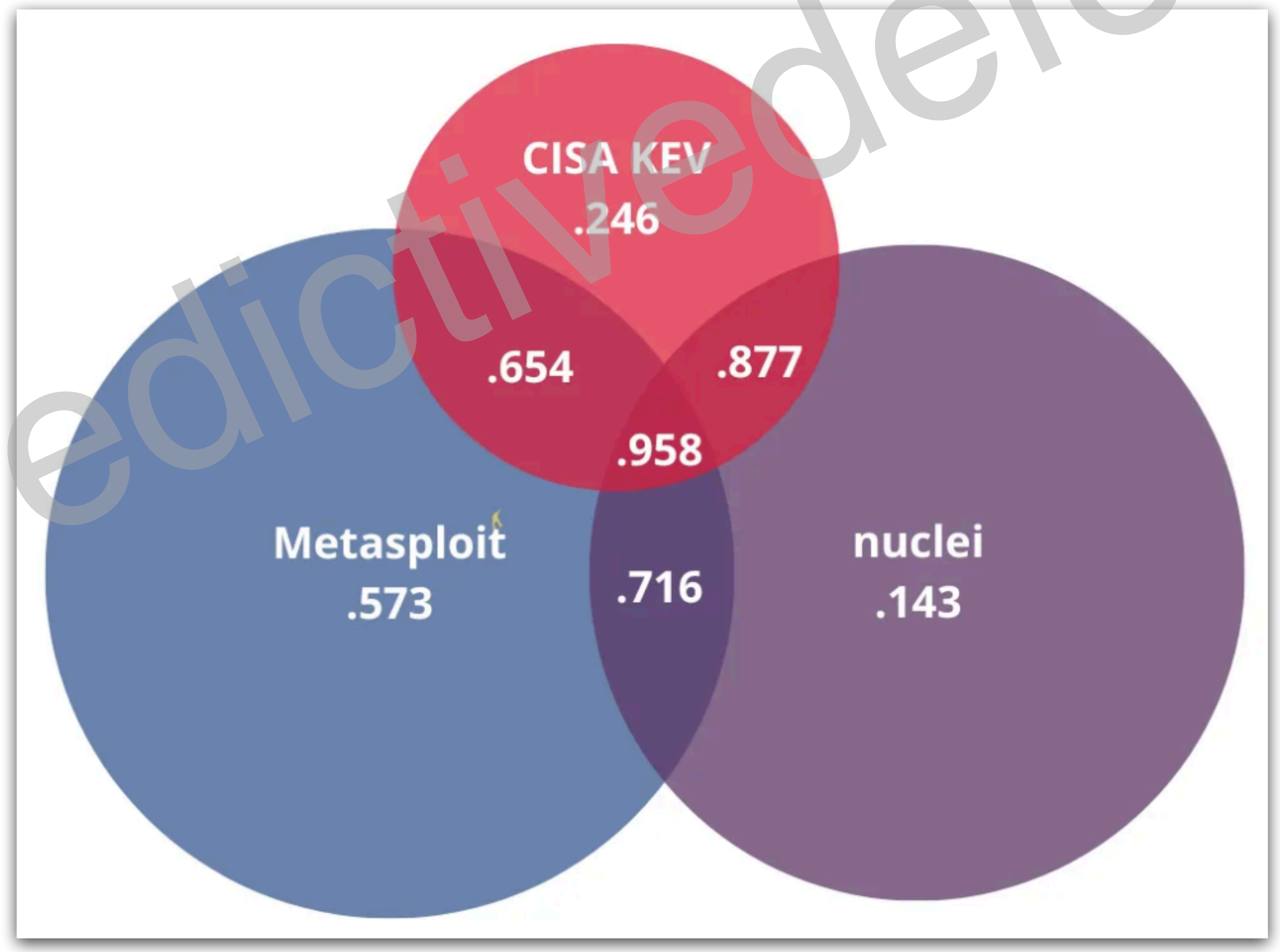


Reference: https://stephenshaffer.io/determining-epss-score-thresholds-for-prioritization-86e08db21798

Mass Exploitation

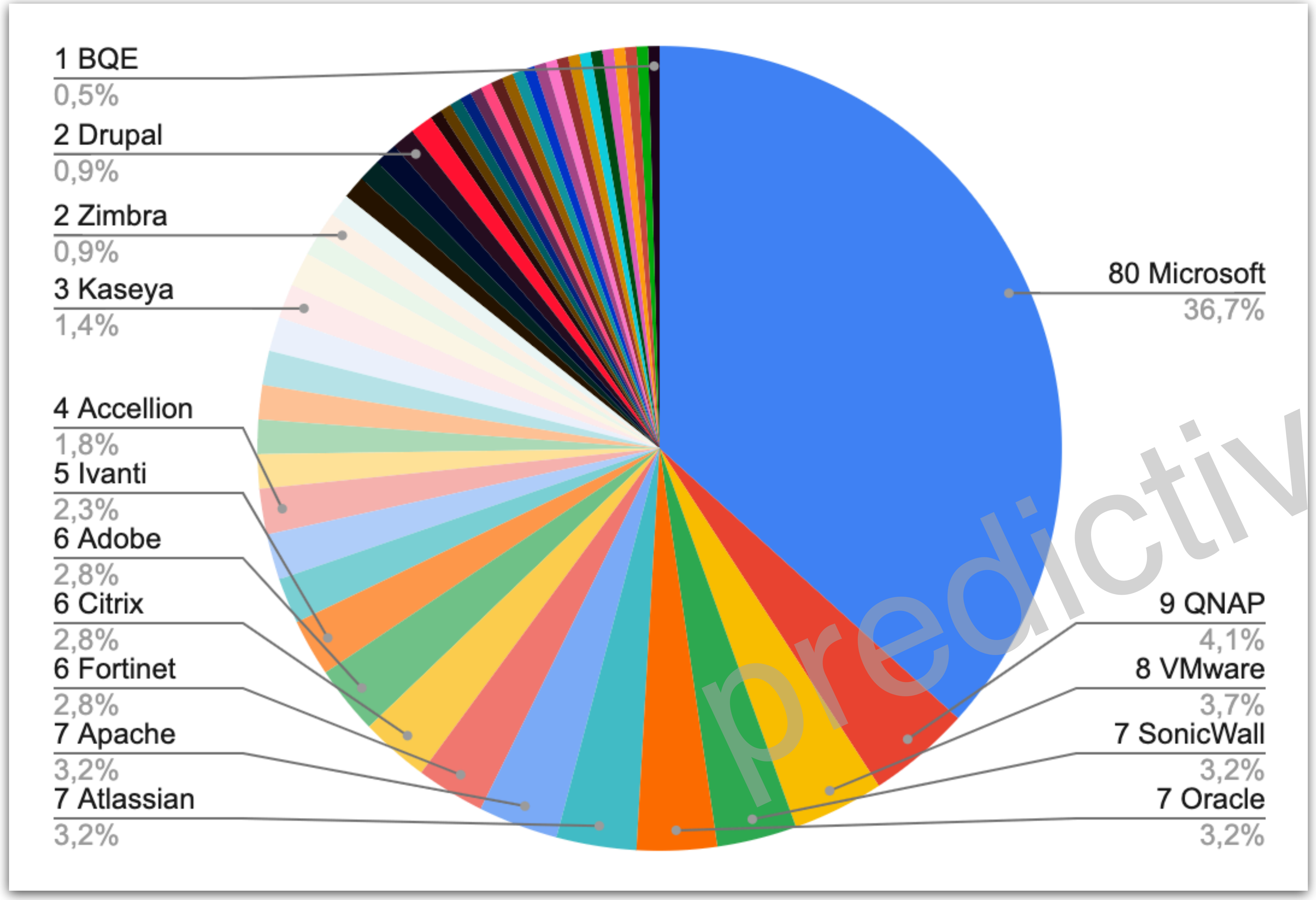
Published exploit code is the strongest contributor to the likelihood of exploitation

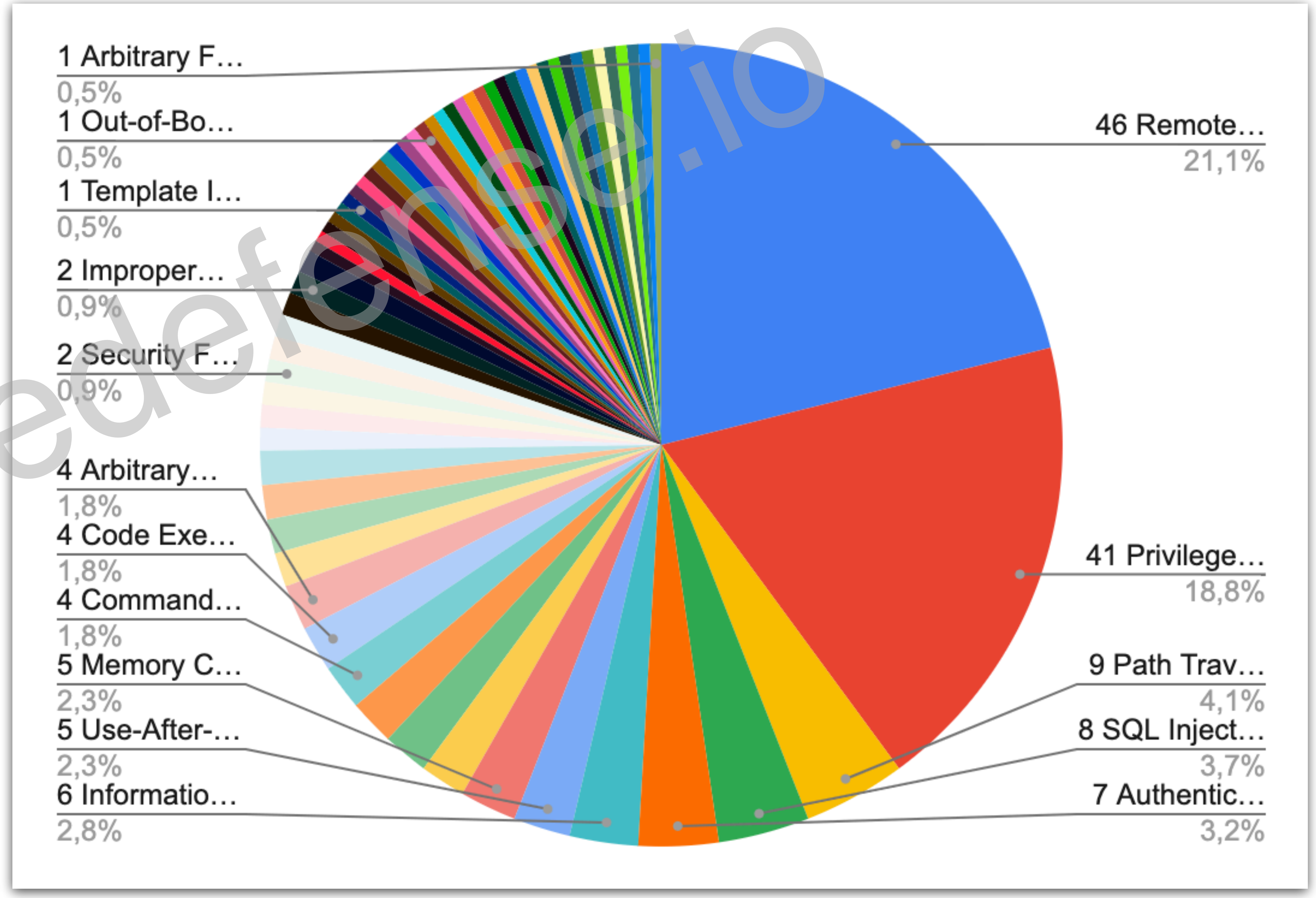
EPSS v1 produced a 37.1% overall exploitation probability when a vulnerability is weaponized which is a 10-fold increase in the likelihood of exploitation activity.



Reference: https://stephenshaffer.io/determining-epss-score-thresholds-for-prioritization-86e08db21798

Ransomware Statistics





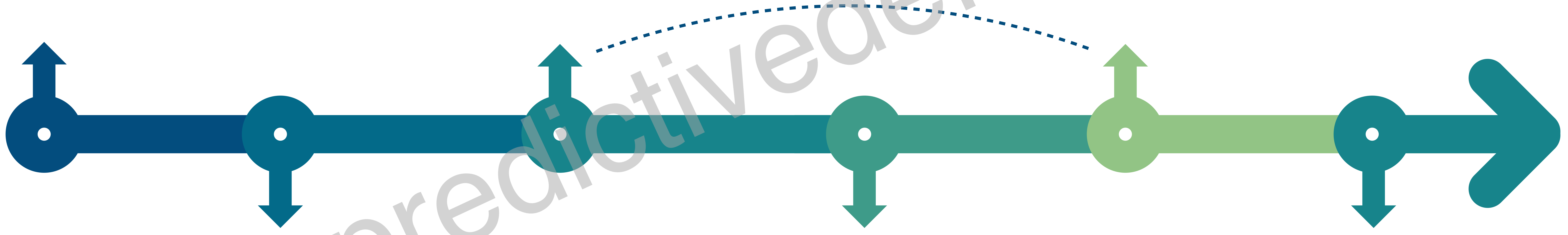
Reference: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

Mass Exploitation

Vulnerability/exploitation intelligence sources

- https://vulners.com/
- https://viz.greynoise.io/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

I&W Analysis



Vulnerability with EPSS > .36

New vulnerability with EPSS score greater than 0.36

Vulners

Exploits are published on Metasploit, Nuclei etc.

Ransomware Keywords

Filter CVE based on the vendor and vulnerability type

Greynoise

New tags are created for the vulnerability

Greynoise

Trending exploit activity for known vulnerabilities

Exploitation

Proactive Incident Response

Proactive Countermeasure Plan: Mass Exploitation

THREAT LEVEL	DEFINITION	MEASURES
LEVEL 0	Weaponised vulnerability with an EPSS score higher than 0.36	Prioritise and fast-track any available patches for the vulnerable systems
LEVEL 1	Vulnerable product and type of vulnerability aligns with those commonly exploited by ransomware groups	1. Deploy IDS signatures tailored to the identified vulnerability 2. Proactively gather intelligence on the latest TTPs used by ransomware attackers for enhanced threat hunting
LEVEL 2	Greynoise has added tags for the new vulnerability (indicating expected exploitation)	1. Conduct a targeted drill or tabletop exercise focused on the new vulnerability to prepare the team for potential ransomware scenarios 2. Increase the depth of monitoring, looking specifically for ransomware indicators of compromise
LEVEL 3	Increased exploitation activity is observed by honeypots (Greynoise or others)	1. Implement emergency patches or workarounds as recommended by vendors or security advisories 2. Tighten access controls and implement network segmentation to limit the spread of potential ransomware infection 3. Activate the incident response team to be on high alert

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 Nation-State

Forecasting

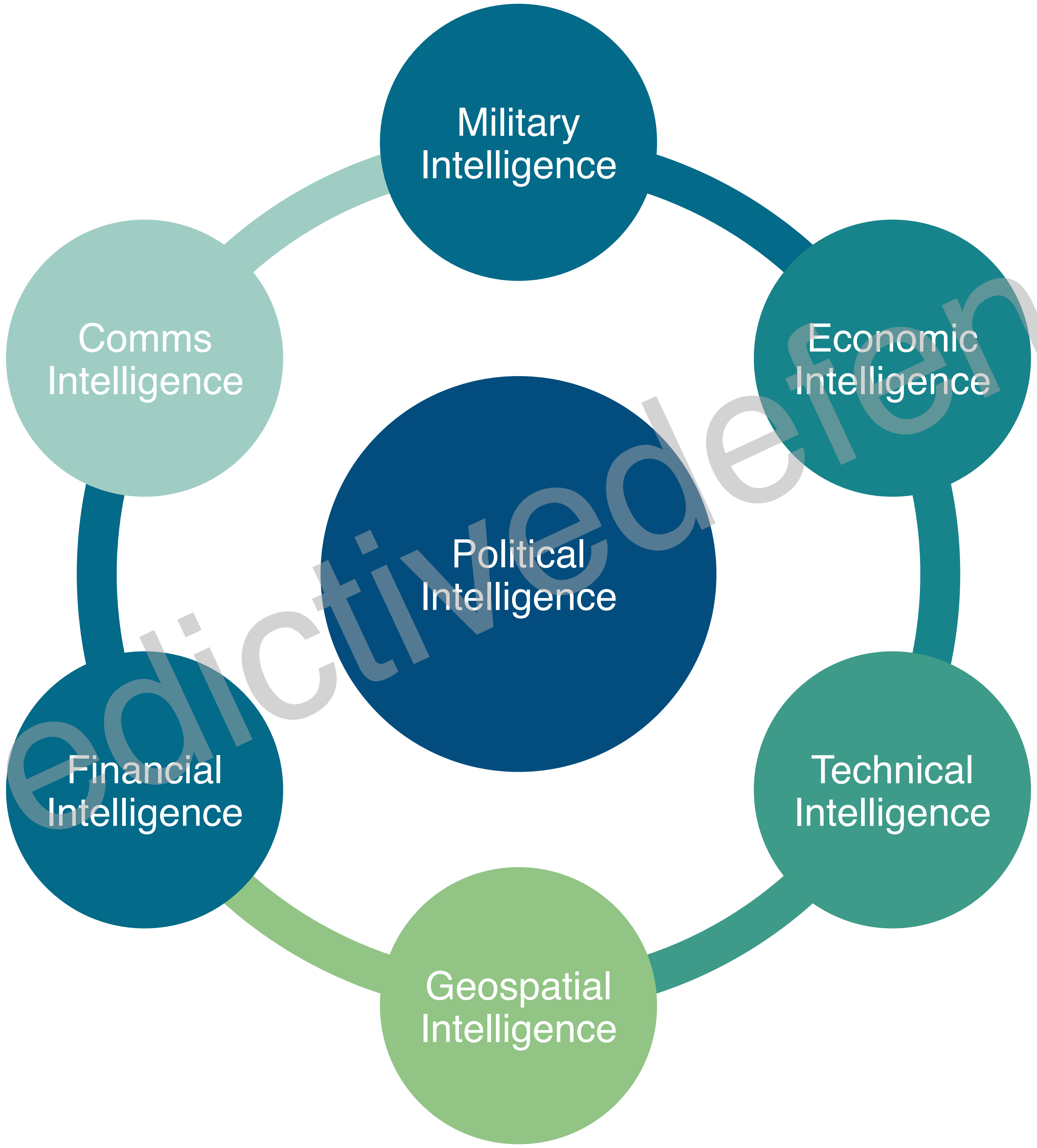
- Assessment of “what’s next?” in long term (1+ year)
- Ideally should inform security leadership decisions so the organization is better positioned against future threats.
- Some analytic frameworks from traditional intelligence analysis: PESTLE-M, DIMEFIL, STEMPLES+

Geopolitical Cyber Risk Analysis

Military and Intelligence Activities in Cyberspace

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.

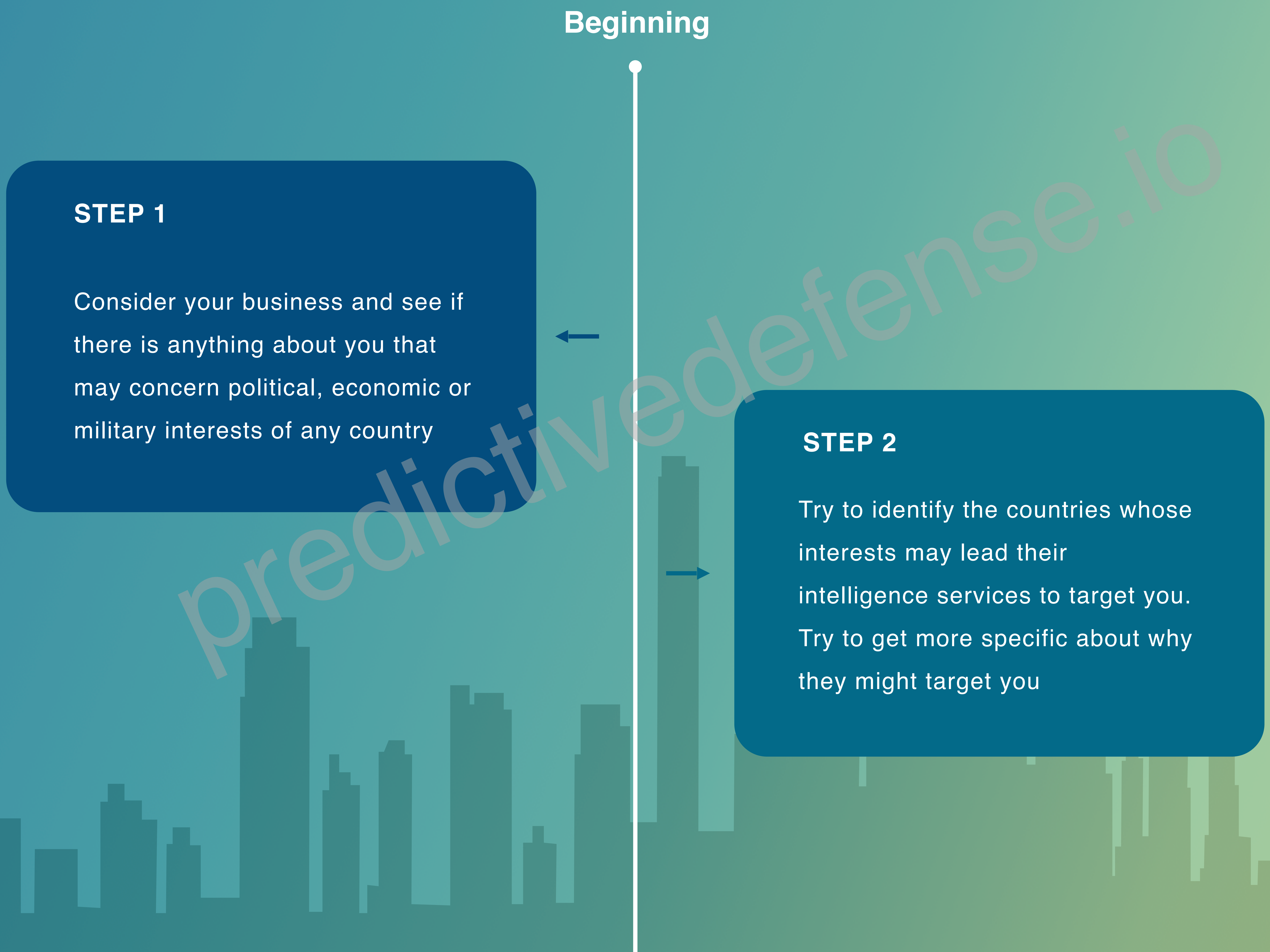
STRATEGIC COLLECTION

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

Questions for Risk Assessment

CATEGORY	RISK SCALE
Political Intelligence	• Does my organization contribute to the policy-making of our home country? • Is my organization involved in activities related to our country's foreign policy? • Does my organization have individuals influential in policy-making within our organization? • Do any of the companies my organization is in business with meet any of the above conditions?
Economic Intelligence	• Does my organization engage in significant export activities? • Does my organization conduct business activities outside our home country? • Does my organization possess intellectual properties that provide a significant commercial advantage? • Is my organization a publicly traded company with a high volume of trade? • Does my organization provide products or services to governments of other countries? • Do any of the companies my organization is in business with meet any of the above conditions?
Communications Intelligence	• Is my organization a provider of communication products or infrastructure? • Does my organization have government agencies among our clients? • Do any of the companies my organization is in business with meet any of the above conditions?

Questions for Risk Assessment

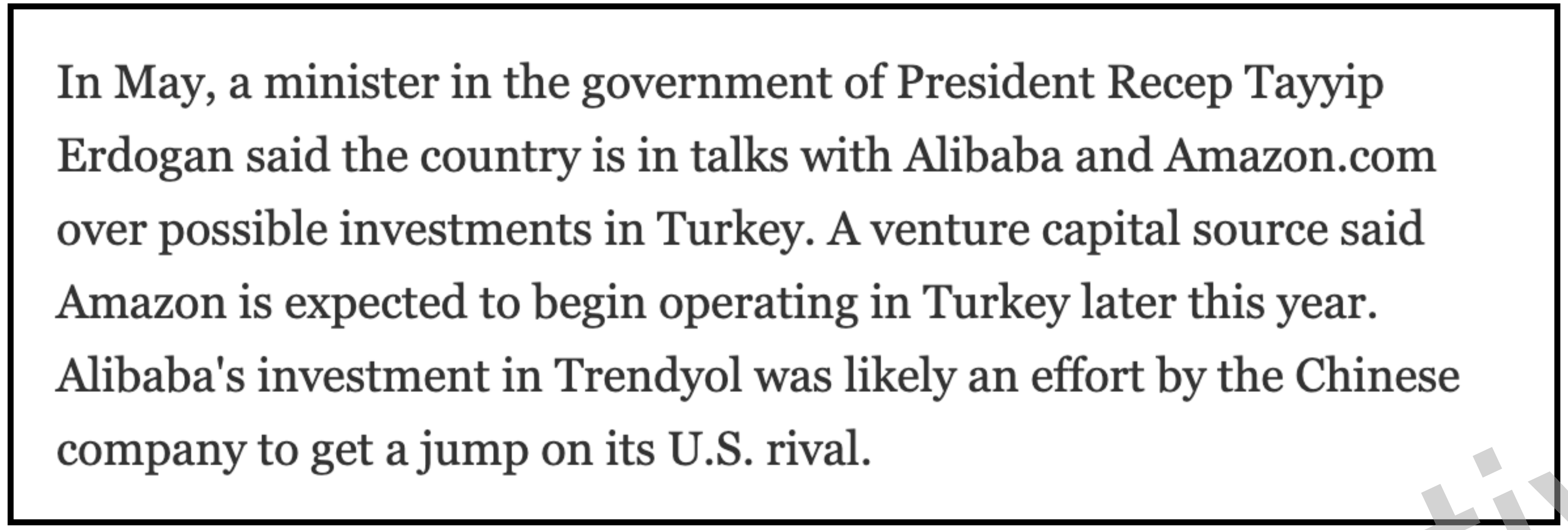
CATEGORY	RISK SCALE
Financial Intelligence	• Is my organization a provider of financial transaction products or infrastructure? • Do any of the companies my organization is in business with meet any of the above conditions?
Geospatial Intelligence	• Does my organization's product or service collect location data from users? • Does my organization process geographic or imagery data? • Do any of the companies my organization is in business with meet any of the above conditions?
Technical Intelligence	• Does my organization conduct research and development in science and technology? • Is my organization's research and development directed towards an active market? • Does my organization's research and development topic have military applications? • Are there other countries investing in the same field as my organization? • Do any of the companies my organization is in business with meet any of the above conditions?

Questions for Risk Assessment

CATEGORY	RISK SCALE
Military Intelligence	• Does my organization develop or contribute to the development of products, systems, or services for military use? • Is my organization a provider of widely used communication infrastructure? • Does my organization own patents or intellectual properties that could be used for military purposes? • Does my organization conduct technological research that could be used for military purposes? • Do any of the companies my organization is in business with meet any of the above conditions?

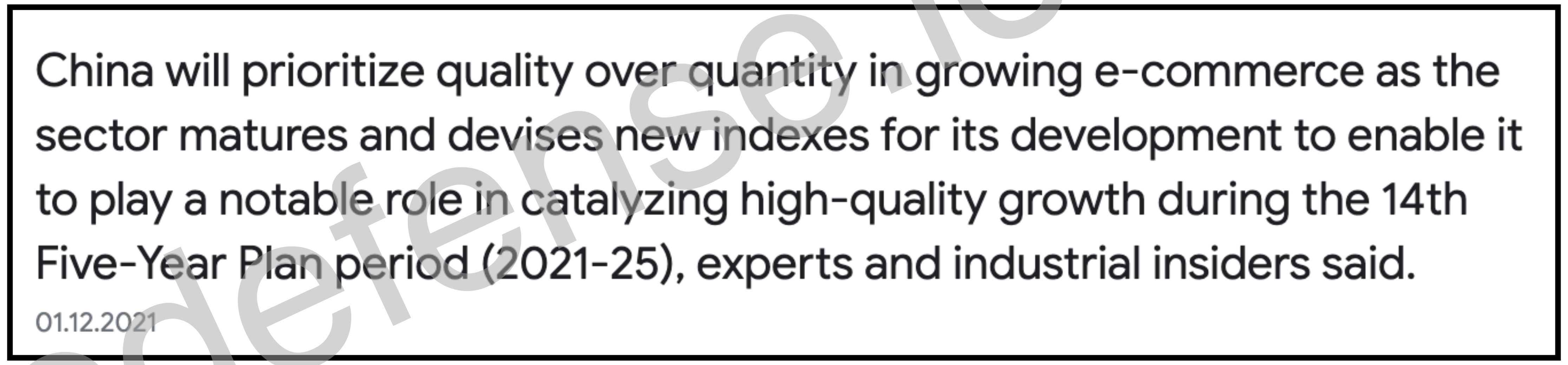
China's Foreign Investments

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.

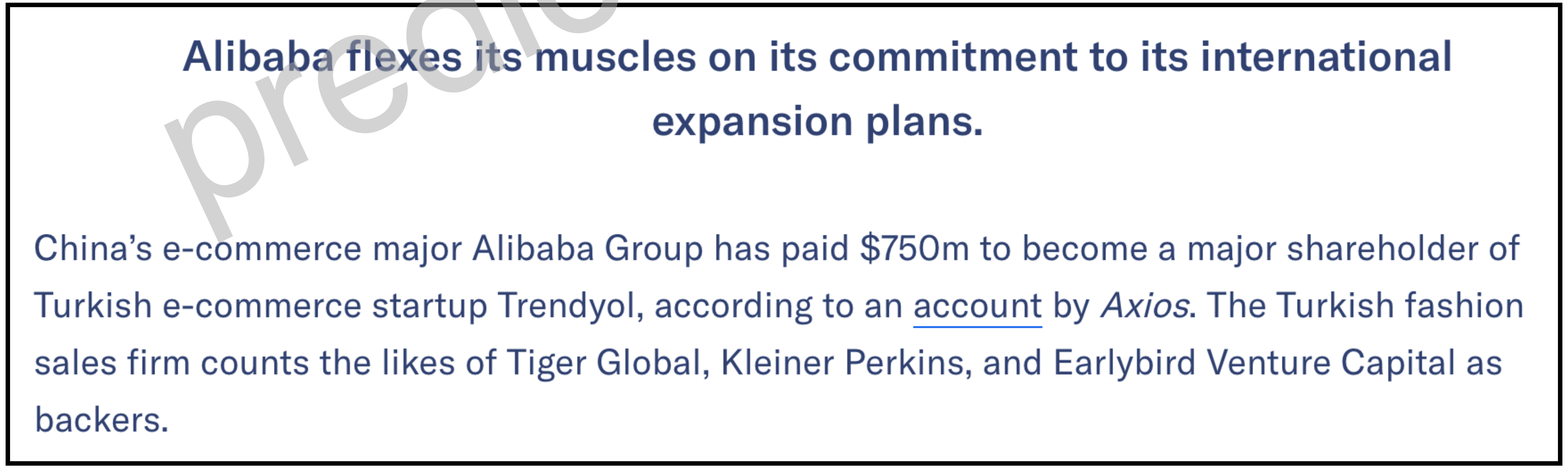
1 Dec, 2021



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

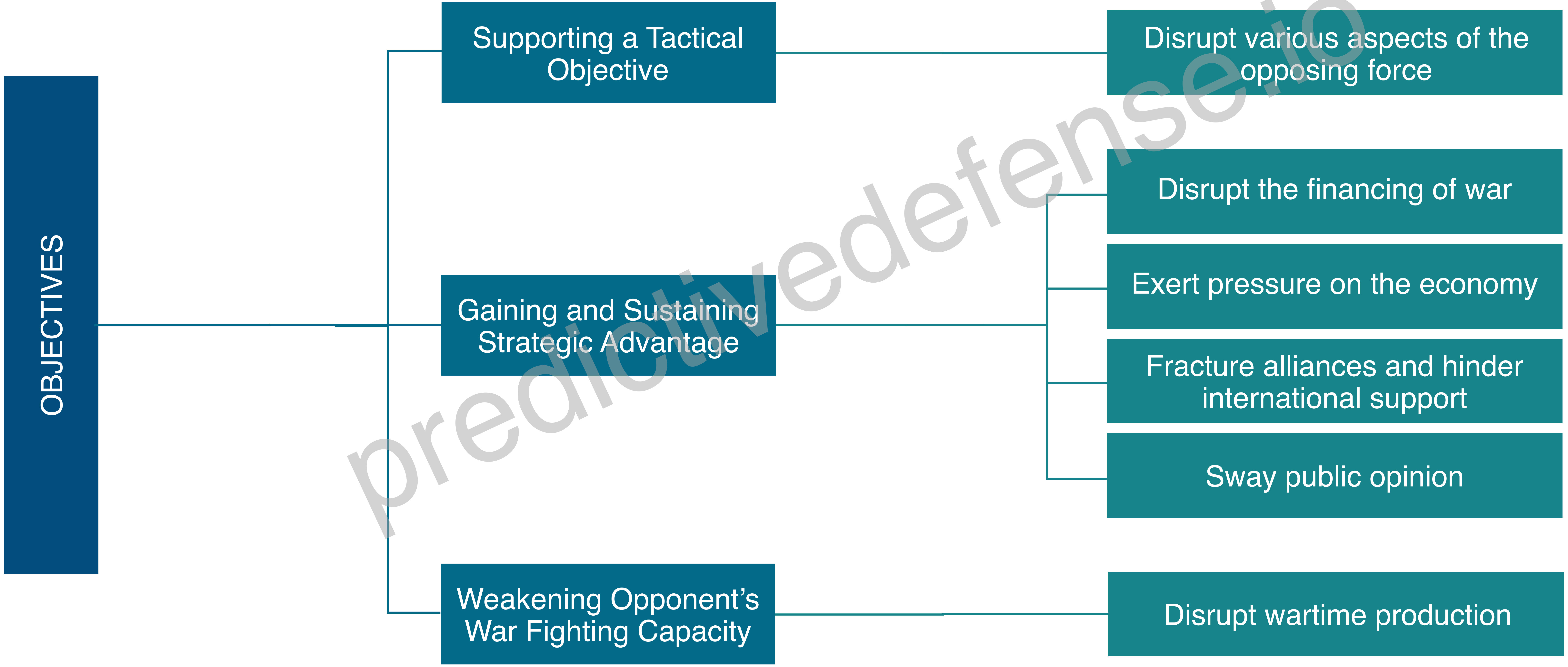


Alibaba flexes its muscles on its commitment to its international expansion plans.

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.

Military Use of Cyberspace

Wartime Support Activities

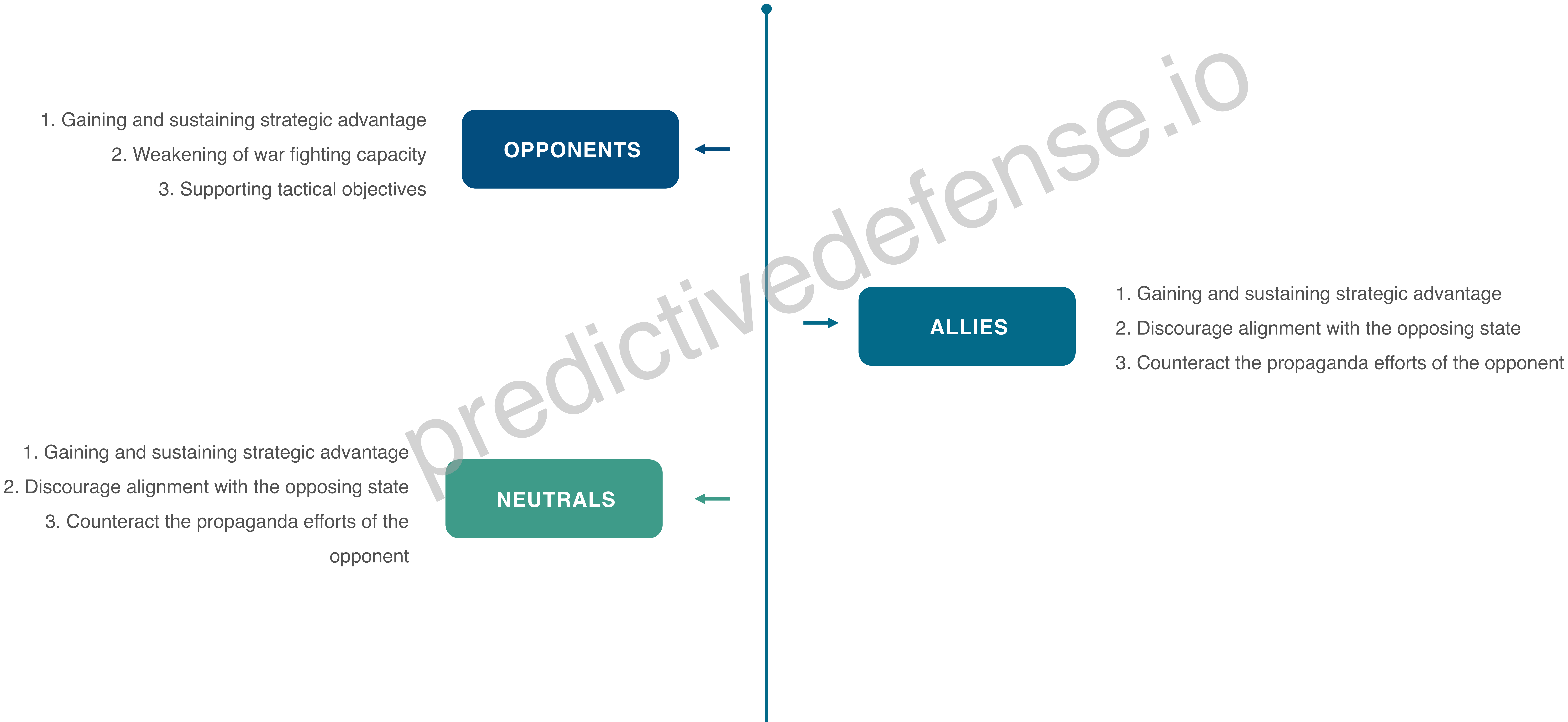

OBJECTIVES
Supporting a Tactical Objective
Gaining and Sustaining Strategic Advantage
Weakening Opponent’s War Fighting Capacity
Disrupt various aspects of the opposing force
Disrupt the financing of war
Exert pressure on the economy
Fracture alliances and hinder international support
Sway public opinion
Disrupt wartime production

Reference: https://robindimyan.medium.com/geopolitical-cyber-risk-cyber-operations-in-modern-warfare-db1392ab0df5

Wartime Support Activities

POSSIBLE CYBER RESPONSES
1. Persistent cyber intrusions targeting gov/mil/intel agencies and their contractors, the defense industry, and think tanks for political, military and technological intelligence
2. Persistent disruptive attacks targeting primary economic industries to exert economic strain (e.g: energy, banking and finance, tourism, manufacturing, large private companies)
3. Persistent disruptive attacks targeting media outlets and communication systems to interrupt the flow of information
4. Persistent disruptive attacks targeting key industries to undermine the material production capability (e.g: chemicals, raw material, aerospace, energy, manufacturing and defense)
5. Coordinated disruptive attacks targeting communication and information networks in support of an ongoing military operation
6. Disruptive attacks targeting primary economic industries or critical infrastructure in retaliation against any perceived political, economic or military support for the opponent state
7. Disruptive attacks targeting media outlets, large private companies, and prominent individuals that publicly support the opponent state to discourage public support

Hierarchy or Targets



OPPONENTS

1. Gaining and sustaining strategic advantage
2. Weakening of war fighting capacity
3. Supporting tactical objectives

ALLIES

1. Gaining and sustaining strategic advantage
2. Discourage alignment with the opposing state
3. Counteract the propaganda efforts of the opponent

NEUTRALS

1. Gaining and sustaining strategic advantage
2. Discourage alignment with the opposing state
3. Counteract the propaganda efforts of the opponent

Russo-Ukrainian War

Review the following material:

- Military Cyber Operations
- Cyber Risk Analysis of Ukrainian Hacktivist Attacks
- Cyber Espionage

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