Vigilocity

Continuous Material Breach Monitoring & Telemetry

Overview Presentation | 05.09.2024

Inspiration Meets Opportunity

“If his forces are united, separate them. If sovereign and subject are in accord, put division between them. Attack him where he is unprepared, appear where you are not expected .” - Sun Tzu

Founder & CEO

Karim Hijazi

- Founder and Chief Executive Officer at Vigilocity
- Founder, Chairman and CEO at Prevailion, a Compromise Intelligence company, transforming the way organizations approach risk mitigation and business decision-making
- Former Director of Intelligence at Mandiant, part of the team that discovered and produced the groundbreaking APT1 report, for the first time publicly attributing cyber attacks to a nation-state actor
- Founder & CEO of Unveillance, researching and developing solutions to mitigate and understand cyber threats through data-driven analysis. Acquired by Mandiant
- Regular appearances on CNN, MSNBC as subject expert when major cyber incidents occur
- Investor and Keynote Speaker

The Problem

Despite deploying the most advanced defensive technologies, organizations still:

- Are infiltrated by advanced malware and malicious reconnaissance tools
- Don’t know the cyber contagion status of their supply-chain and 3rd parties
- Are at an asymmetric disadvantage against sophisticated threat actors
- Lose critical time with hunting through false positives and IOC data lakes

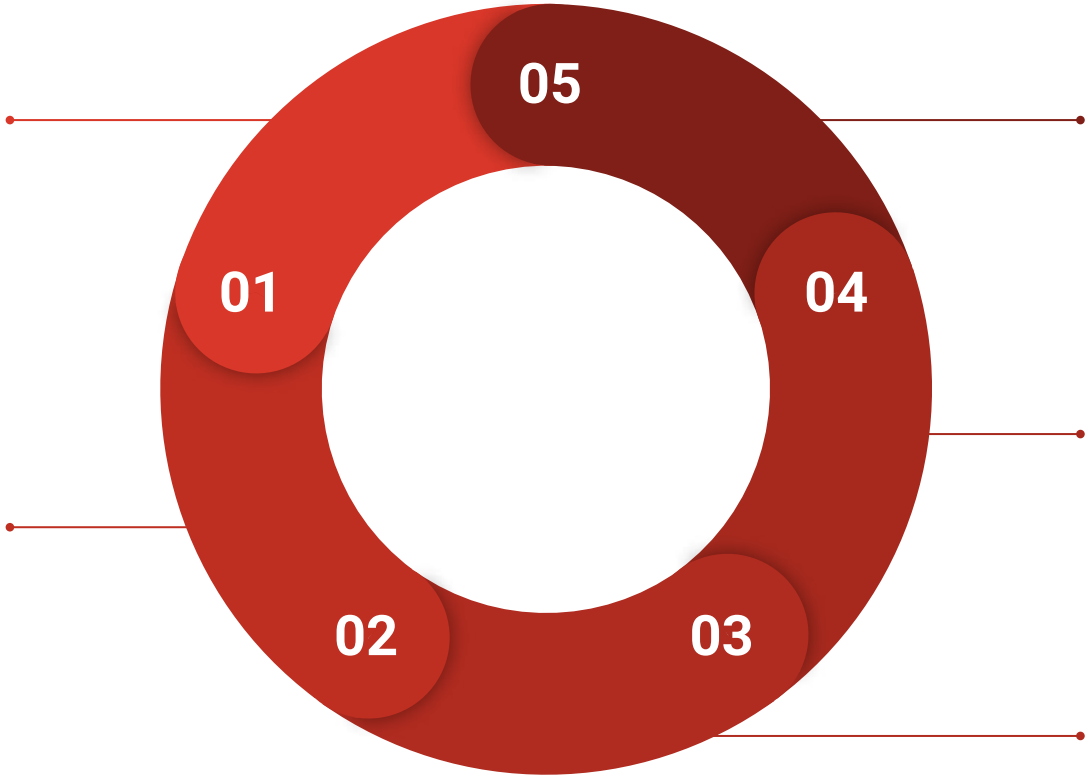
Anatomy of the Attack

Phishing & Initial Compromise

Threat actors begin their attack campaign by socially engineering unsuspecting victims (company employees and trusted contractors) with convincing emails, sms messages or even phone calls.

Lateral Movement & Reconnaissance

Users are convinced to click on links to malicious websites where malware is downloaded to their device. The malware then looks for other devices to infect on the network and shares critical information with it's operator through a command and control (C2) channel.



Reputation Impact, Identity Theft & Downtime

The resulting impact not only costs the target financially, but can also be damaging to reputation and customer and stakeholder confidence.

3rd Party & Expansion & Infection

In addition to impacting the intended victim, the malware will spread through trusted connections to partners as well.

Stage Escalation & Ransomware Deployment

Once the operator has received enough information about the intended target's network, resources, back-ups and employees, they will deploy custom software to encrypt all or part of the target's critical systems rendering them inoperable.

The Problem Is Massive and Growing

76% "In 2022, 76% of organizations were targeted by a ransomware attack, out of which 64% were actually infected. Only 50% of these organizations managed to retrieve their data after paying the ransom. Additionally, a little over 66% of respondents reported to have had multiple, isolated infections." - CSO Online

"Cybercriminals mostly abused Microsoft's brand name in phishing attacks, with more than 30 million messages using its branding or mentioning products like Office or OneDrive. However, other companies were also frequently impersonated by cybercriminals, including Amazon (mentioned in 6.5 million attacks); DocuSign (3.5 million); Google (2.6 million); DHL (2 million); and Adobe (1.5 million)." - Lookout

30M

$10.5T "The cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025." - Cybersecurity Ventures

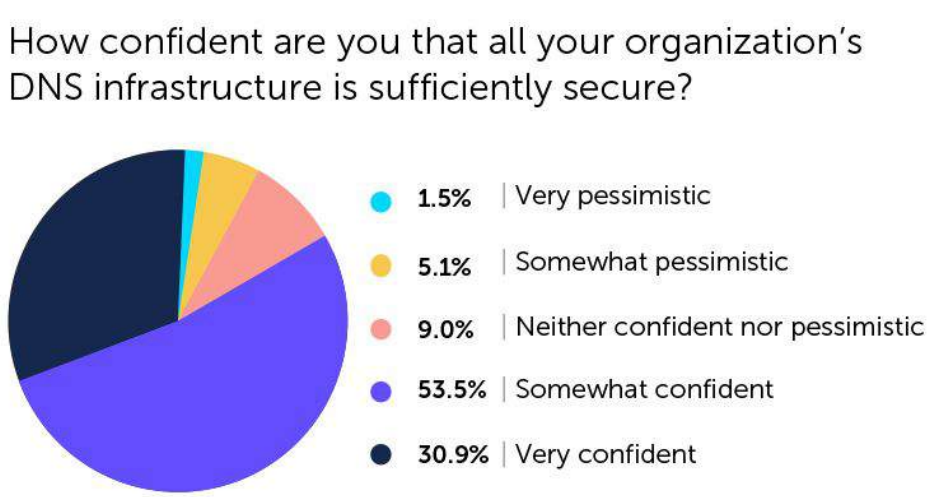
2024 Security & Exchange Commission Cyber Breach Disclosure Rule

What must be disclosed? The final rule requires public companies to disclose the occurrence of a material cybersecurity incident and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations **within four business days**. This disclosure is focused on the material impacts of a material cybersecurity incident. It is narrower than what the Commission originally proposed, which would have required additional details that were not explicitly limited by materiality. In revising the disclosure requirement, the Commission took into account not only the company's compliance costs but also its need to respond and remediate incidents.

https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

Market Size

The global DNS security software market size was USD 995.8 million in 2021 and is projected to touch USD 2377.86 million by 2031, exhibiting a CAGR of 9.1% during the forecast period



https://bluecatnetworks.com/blog/security-automation-cloud-integration-keys-to-ddi-solution-success/

https://www.businessresearchinsights.com/market-reports/dns-security-software-market-100448

The Opportunity

A continuously monitoring platform that disrupts threat actors, as and when, they begin to establish their infrastructure and **materially** breach organizations and governments.

- Zero software, hardware or configuration changes required
- Empirical evidence of supply-chain and third-party cyber contagion risk
- High fidelity signal intelligence with low to no false positives

The Product

Vigilocity presents Mythic©, a comprehensive SaaS platform focusing on threat actor infrastructure interdiction and material breach detection. Key aspects of the platform include:

- Operational without any hardware, software, or installation prerequisites.
- Groundbreaking capabilities for mitigating supply chain and third-party risks, particularly beneficial for cyber insurance and M&A scenarios.
- Unparalleled empirical evidence intelligence for actuarial modeling and comprehensive cyber due diligence.

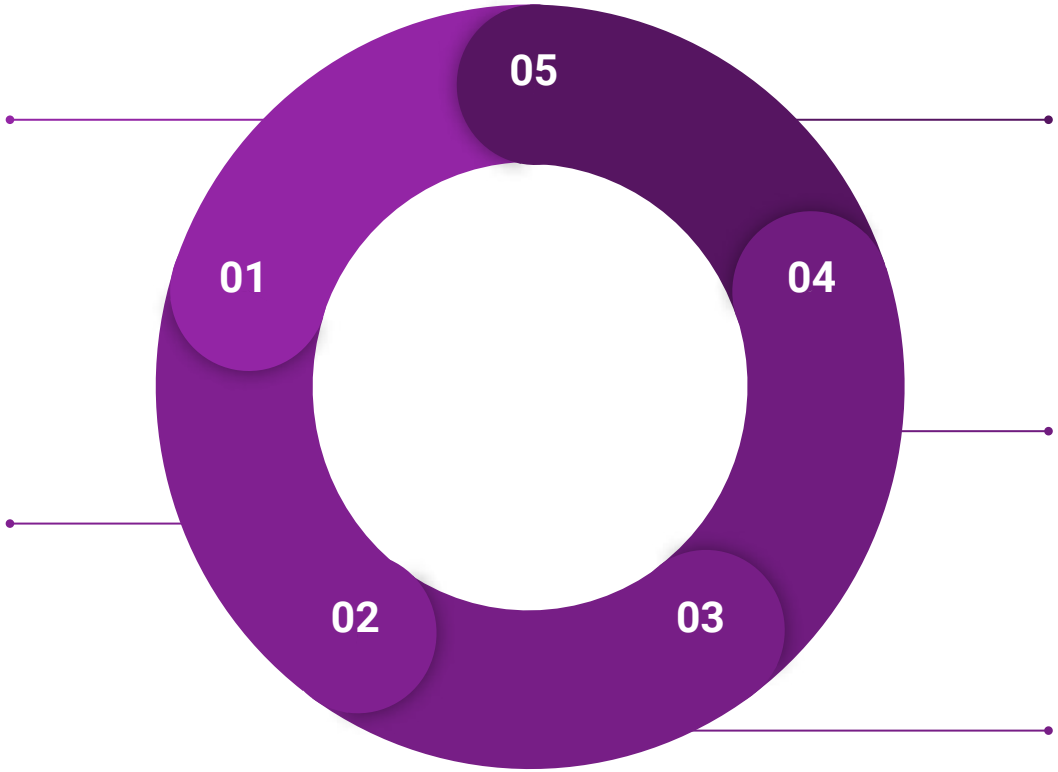
The Methodology

Domain Registration Information Ingest

Domains with unmasked and unredacted domain registration information is collected daily from nearly 1000 global registrars.

Automated Threat Analysis

All domains are automatically analyzed against both open source threat intelligence as well as Vigilocity's own proprietary hunt database.



Payload & Material Breach Confirmation

Once a DNS query has been received, Vigilocity Internet nodes respond with a ephemeral IP address and complete a full TCP (Layer 7) handshake with the live malware.

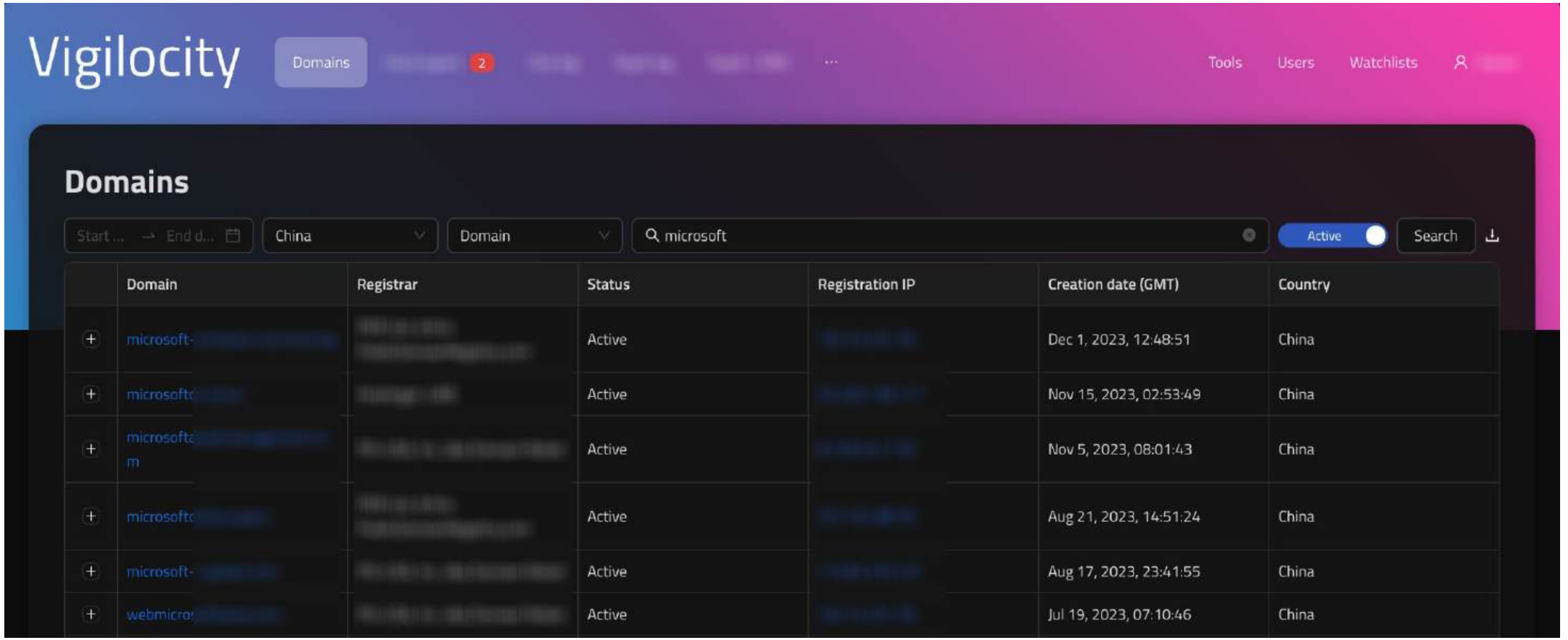
DNS Telemetry Collected

Once the registrars alter the authoritative DNS setting for the convicted domains, Vigilocity begins to collect DNS queries to the now "double-agent" domains.

Domain Conviction Queued

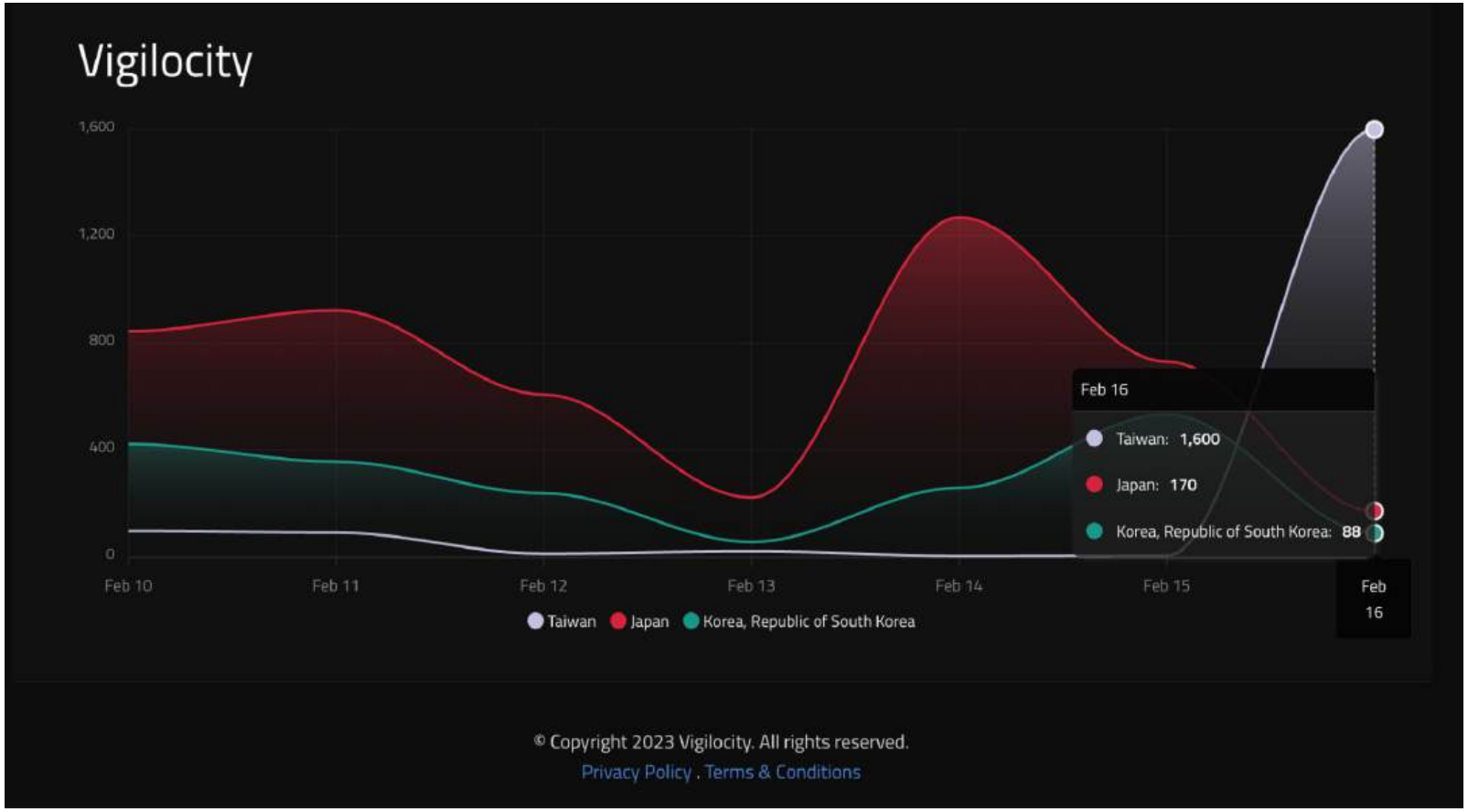
Domains that meet a strict criteria and deemed as high confidence malicious command and control domains are submitted to a conviction queue from where the registrars then review and take action.

Precognitive Threat Analysis



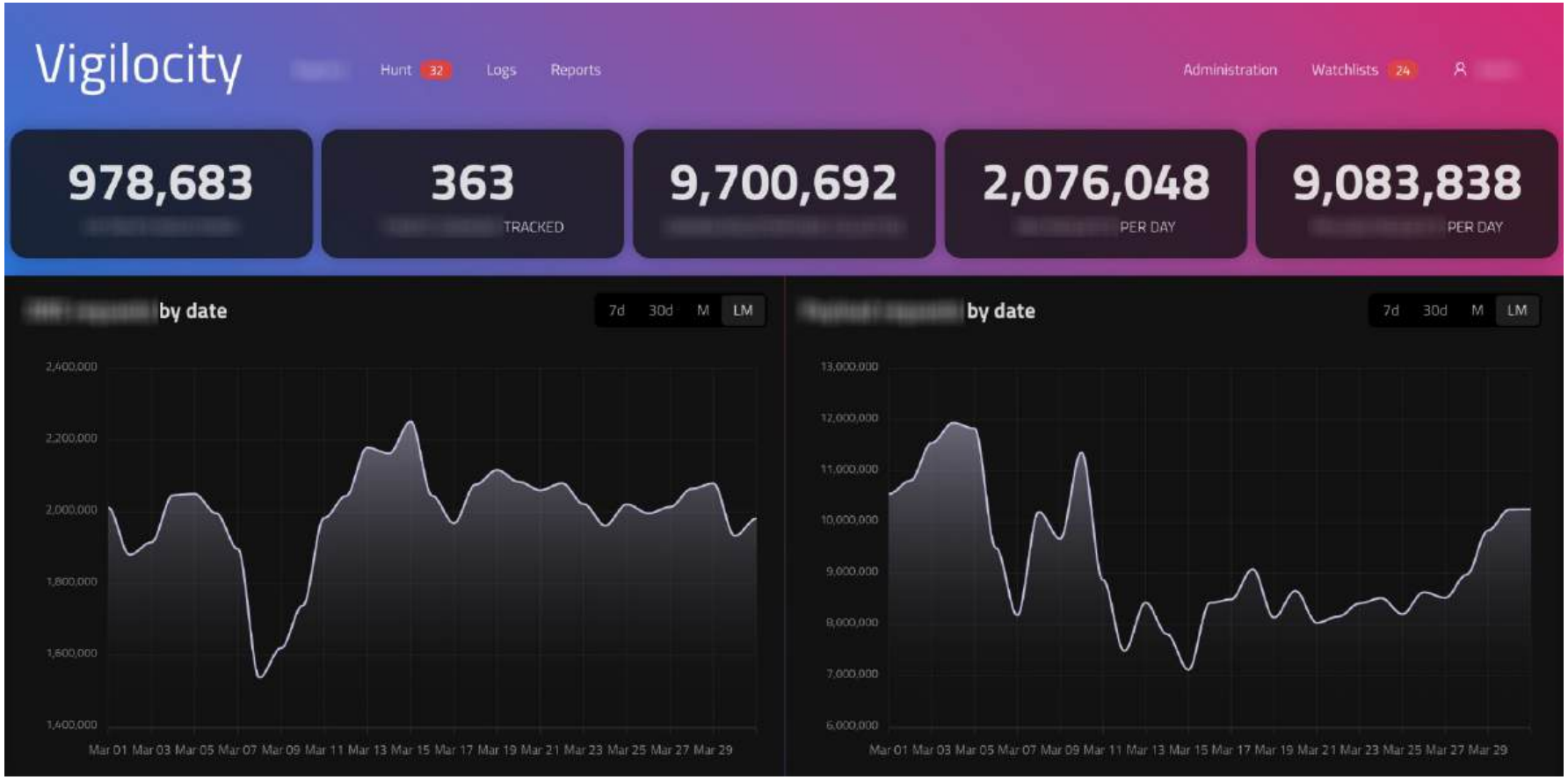
Identify ransomware and phishing campaigns in their earliest stages.

Global Breach Analysis



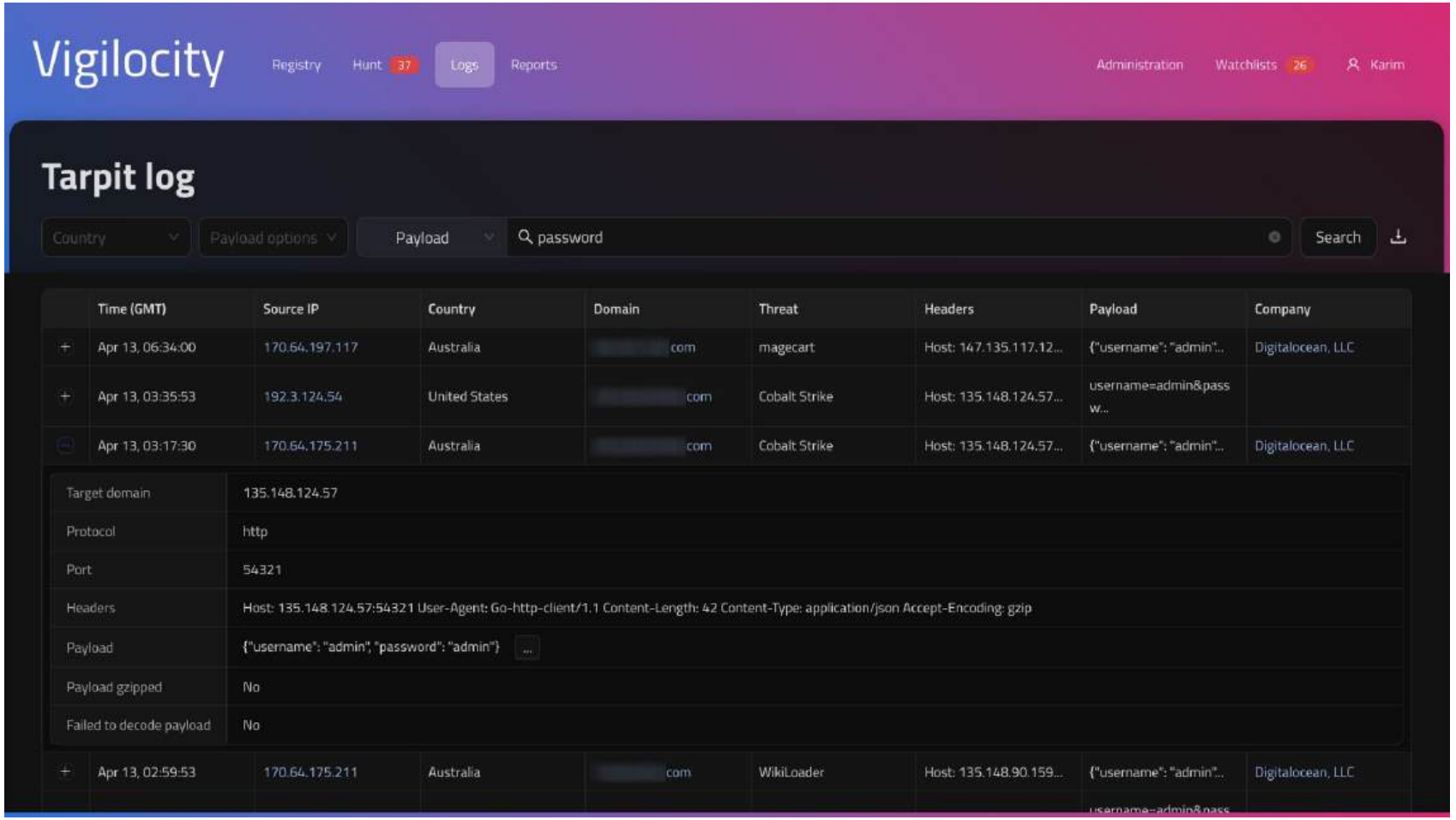
Witness emerging malicious trends on a global scale.

Real-Time Compromise & Breach Intelligence



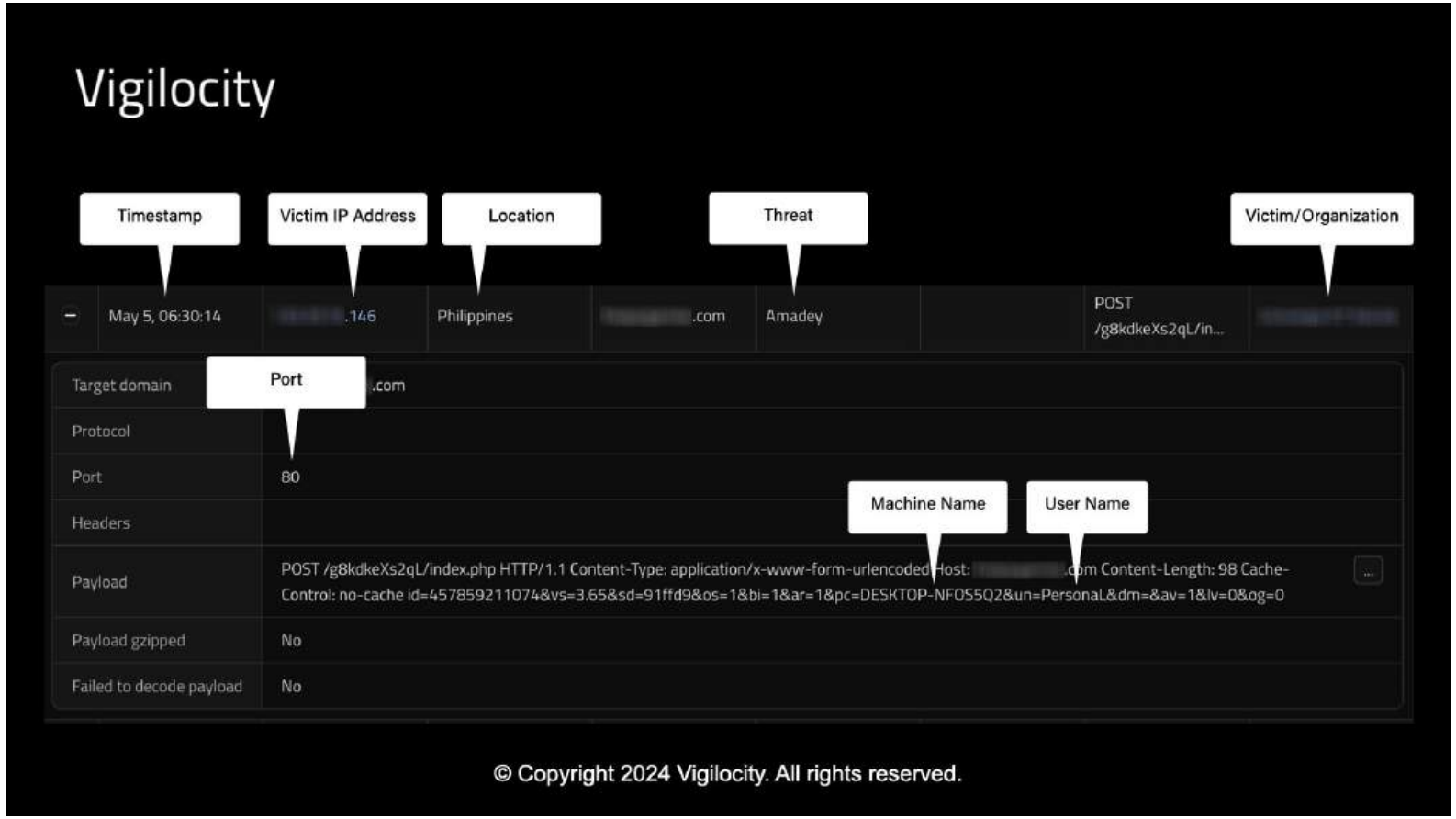
Witness frequency, cadence, and velocity of live and historical malware infections

Active Payload Capture & Analysis



Identify actual payload exfiltrated by active malware infections qualifying materiality of breach

Actionable Alerting



- Timestamp
- IP Address
- Threat Family
- C2 Domain
- Protocol
- Port
- Headers
- Payload
- Victim Organization
- Country

Vigilocity delivers critical intelligence necessary to mitigate an attack in its earliest stages.

By The Numbers

10 Years +
Historical Data

40 Million +
Email Addresses

10 Million +
Collected Payloads

36 Million +
Domains Tracked

470K +
Geolocations

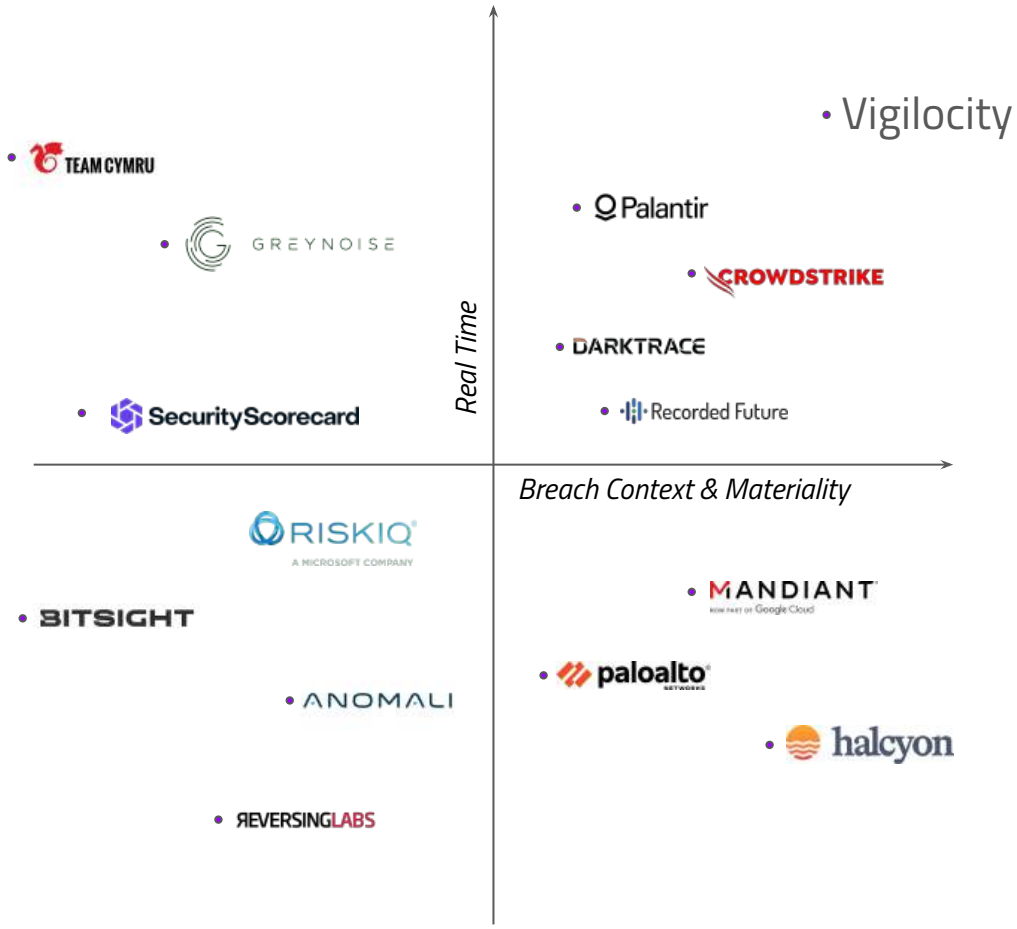
50M +
IP Addresses

30 Million +
Registrants Tracked

6000 +
Data Sources

$540 Million +
Identified Infrastructure
(Minimum)

A Clear Market Need



Real Time:

In today's hyperconnected world, where threat actors escalate attacks at unprecedented speeds, real-time cyber intelligence is indispensable. It provides instant insights into evolving threats, enabling swift countermeasures to protect businesses, governments, and individuals.

Breach Context & Materiality:

Now, more than ever, the market needs breach context to navigate the overwhelming flood of false positive IOCs and flawed threat intelligence. Breach context offers clarity amidst the noise, helping organizations prioritize and respond effectively to genuine threats, minimizing the risk of costly breaches.

Case Study - Third-Party Partner & Supply-Chain Risk Management

Challenge:

Coca-Cola faced significant cyber risks due to its expansive supply chain network. With suppliers, distributors, and partners spanning across the globe, the company was exposed to various vulnerabilities in its digital infrastructure. Cyberattacks targeting any point in the supply chain could disrupt operations, compromise sensitive data, or even result in product tampering.

Solution:

Vigilocity addressed Coca-Cola's supply-chain cyber risk by implementing a comprehensive solution for continuously monitoring all organizations within Coca-Cola's supply chain for active and historical malware infections. By partnering with Vigilocity, Coca-Cola ensured the integrity of its operations, safeguarded sensitive data, and maintained consumer trust in its products.

Case Study - Cyber Insurance & Actuarial Modeling

Challenge:

In the wake of increasing cyber threats, Tokio-Marine HCC encountered the critical need to discern which of their insured customers were most susceptible to phishing and ransomware attacks. They were tasked with devising a comprehensive approach to evaluate the vulnerability levels of their diverse clientele accurately. This challenge demanded a nuanced understanding of various risk factors, including industry-specific threats and the effectiveness of existing protective measures.

Solution:

By meticulously analyzing both historical and active compromise statuses of their insured customers, Vigilocity provided invaluable insights into the cybersecurity landscape. This proactive approach enabled Tokio-Marine HCC to prioritize risk mitigation efforts, tailor preventive measures, and ultimately fortify the resilience of their insured customers against cyber threats.

Case Study - M&A Cyber Due Diligence

Challenge:

EY Parthenon required a more robust method of cyber due diligence for their clients interested in conducting a deeper analysis of their potential acquisition targets that would go beyond the conventional vulnerability assessment and self-attestation scoring widely available and generally inaccurate.

Solution:

Vigilocity delivered crucial insights into the cybersecurity posture through rigorous examination of the historical and current compromise statuses of the target acquisitions of EY Parthenon's clientele for due diligence purposes. This proactive strategy empowered EY Parthenon to accurately advise their clients and in many cases provide powerful financial leverage during negotiations.

Case Study - Threat Context & Material Breach Intelligence

Challenge:

Netwitness faced a pressing need for elevated threat intelligence that transcended the limitations of conventional indicators of compromise (IOCs). As cyber threats evolved in complexity and sophistication, relying solely on traditional IOCs proved insufficient in detecting and mitigating emerging risks effectively. Netwitness recognized the imperative for a more nuanced and comprehensive approach to threat intelligence to stay ahead of adversaries.

Solution:

Vigilocity's high-fidelity material breach intelligence solution provided Netwitness with the precise threat context and high signal-to-noise ratio they required. By focusing on actual breaches and incidents, Vigilocity offered actionable insights tailored to Netwitness' needs, enhancing their understanding of evolving threats and enabling more accurate detection and response capabilities.

Case Study - Security Controls Validation & Monitoring

MUBADALA

Challenge:

Mubadala, as a global investment company with diverse interests, requires a robust security validation solution to protect its assets and data from evolving cyber threats. With operations spanning multiple sectors, including aerospace, energy, and healthcare, a comprehensive validation solution was vital to assess and enhance security infrastructure, ensure regulatory compliance, and maintain stakeholder trust.

Solution:

Vigilocity offered Mubadala a unique zero-touch approach to security validation, actively testing security controls without disrupting operations. This approach enhanced security while minimizing operational overhead, providing an efficient solution to tune and strengthen Mubadala's defenses against evolving cyber threats.

Case Study - Country/Government Proactive Security

Challenge:

STC (Saudi Telecom) had a mission-critical need to shield the Kingdom of Saudi Arabia from rising cyber threats. As technology evolved, so did the methods of attackers, posing risks to national security. STC sought a preemptive solution to anticipate and neutralize emerging threats and fortify the Kingdom's digital defenses, ensuring resilience against malicious intrusions and cyberattacks.

Solution:

Vigilocity played a pivotal role in enhancing Saudi Arabia's cybersecurity posture by providing proprietary intelligence on pre-weaponized threat infrastructure. This proactive approach enabled the Kingdom to mitigate risks before they could establish a foothold. Leveraging Vigilocity's insights, Saudi Arabia preemptively identified and neutralized potential cyber threats, safeguarding critical infrastructure and national security.

Technology Roadmap Overview

	2024	2025
Q1	TLS Decryption	Automated Malware Destruction
Q2	Comprehensive Public API	Counter-Ransomware
Q3	Third-party Risk Prediction	Digital Dye-Pack v1.0
Q4	Partner Integrations	Cyber Insurance Policy Creation

Summary

- Organizations and governments alike face an ever-increasing threat from sophisticated threat actors despite deploying best-in-class cybersecurity technology
- Vigilocity delivers timely groundbreaking capabilities for mitigating supply chain and third-party risks, particularly beneficial for cyber insurance and M&A scenarios.
- Proven technology, market readiness and GTM velocity

Thank you for your time and kind consideration.

Karim Hijazi - Founder & CEO - karim@vigilocity.com

