ITSEC
SECURITY DELIVERED

AUGUST 2025

ITSEC: CYBERSECURITY SUMMIT 2025 EDITION

ITSECBUZZ

CYBERSECURITY MAGAZINE

CSIRT: Why Your Organization Need to Have One?

The Bangladesh Bank Heist that Shook The World

IntelliBroń Aman: Protect Your Phone from Malicious Threats in Real Time.

ITSEC: Cybersecurity Summit 2025

Indonesia Steps Into The Quantum Era of Cyber Defense

ITSEC
SECURITY DELIVERED

TABLE OF CONTENT

itsec.buzz

Editor-in-Chief:
M. Rasyid Sahputra

Design & Layout:
Z. Ananda
Chatra W.
Zakifuadi

Writers:
Yoko Kho
Herman Fransiskus
Z. Ananda

Proof Reader:
Irra Fachriyanthi

Images Properties:
ITSEC Asia
Envato
Freepik.com
AI Generated

> *Cybersecurity is not just about protecting your devices.* ***It's about protecting yourself.***

ITSEC CYBERSECURITY SUMMIT 2025
The Largest Critical Infrastructure Cybersecurity Event in Southeast Asia

Opening

ITSEC Cybersecurity Summit 2025:

INDONESIA STEPS INTO THE QUANTUM ERA OF CYBER DEFENSE

Jakarta witnessed a historic moment in August 2025 as PT ITSEC Asia Tbk (IDX: CYBR) officially opened the ITSEC Cybersecurity Summit 2025. Over the course of three days, from 26 - 28 August, the city became the center of gravity for the region's most urgent cybersecurity conversations. Carrying the theme "The Largest Critical Infrastructure Cybersecurity Event in Southeast Asia," the summit gathered more than a thousand participants including government leaders, regulators, industry experts, academics, and technology innovators. The mission was clear: to confront the fast-growing wave of cyber threats that put national and regional digital infrastructures at risk.

The program was ambitious in both scale and substance. More than 40 sessions filled the agenda, ranging from keynotes to panels and technical presentations. Each session brought together perspectives from across the ecosystem. Representatives from leading technology and cybersecurity organizations such as Aikido, Mimecast, Segura, BlackDuck, Promon, SOCRadar, Vicarius, Google Cloud, Fortinet, Lucy Security, and Securonix joined the stage, sharing best practices and strategies to safeguard critical sectors. Their insights underscored a shared understanding that defending digital systems today requires both cutting-edge solutions and cross-border collaboration.

The opening day set the tone with senior officials addressing the urgency of building resilience. The National Cyber and Crypto Agency emphasized the importance of awareness and capacity building, noting that cyber resilience can no longer be seen as a task reserved for IT departments alone. It is a shared responsibility across governments, industries, and even individuals who increasingly rely on digital services for daily life. The Ministry of Defense echoed this view, reminding participants that critical infrastructure is tied to sovereignty itself. In a hyperconnected world, ensuring the stability of power grids, healthcare systems, transportation networks, and financial services is as strategic as protecting territorial borders.

What made this year's summit especially compelling was the breadth of topics. Sessions went beyond abstract discussions and explored pressing issues through real-world case studies. Experts presented on malware incidents that had disrupted cruise ship control systems, highlighting the human and economic consequences of cyberattacks on operational technology. In another session, medical systems and hospitals were in focus, underlining the stakes when patient safety depends on secure and reliable data.

The summit also looked forward, addressing what many see as the next great challenge in cybersecurity: quantum computing. While quantum machines hold immense promise for breakthroughs in areas like artificial intelligence and drug discovery, they also have the potential to dismantle today's encryption standards. Public-key cryptography, which underpin

Opening Ceremony
with BSSN & Ministry of Defense RI

Photo: Special Courtesy

secure banking transactions, government communications, and digital certificates, could be rendered obsolete in a matter of seconds once large-scale quantum computers become available. This looming threat drove discussions on post-quantum cryptography and the urgent need for industries to adopt quantum-safe standards.

ITSEC Asia outlined its approach to post-quantum cryptography through three pillars. The first is research and testing, where the company will work with global technology firms and universities to develop proofs-of-concept that validate the security and practical application of quantum-safe algorithms. The second is training and capacity building through the newly launched ITSEC Cyber Academy. By connecting research outcomes to specialized training programs, ITSEC aims to prepare Indonesian IT professionals with the skills required to adopt these new standards. The third pillar is industry awareness, using platforms like the summit to raise understanding about PQC and the urgency of acting before quantum risks move from theoretical to real.

Beyond quantum topics, the summit created space for knowledge-sharing through the Call for Papers program. Industry experts and academics submitted perspectives on both information technology and operational technology environments, with selected works presented during the conference. These papers added intellectual depth and academic rigor to the event, ensuring that discussions were not only practical but also grounded in forward-looking research.

The competitive spirit of cybersecurity also came alive through the Capture The Flag (CTF) competition. This event challenged participants to solve real-world cyber problems under pressure, testing their ability to think critically and respond quickly. For many, it was more than just a contest, it was an opportunity to benchmark skills, gain recognition, and connect with industry professionals who could open doors to future careers.

ITSEC CYB
SU
The Largest Critical Infrastructu
Event in Southeast
ITSEC CYBERSECURITY SUMMIT 2025

Patrick Dannacher
President Director, ITSEC Asia

Conference with Experts

CTF Competition Winner

Activity

Photo: Special Courtesy

Photo: Special Courtesy

As discussions unfolded, one common thread emerged. The digital economy of Southeast Asia is growing at breakneck speed and is projected to reach $1 trillion in gross merchandise value by 2030 (*source: World Economic Forum). This growth will only be sustainable if the region's cybersecurity keeps pace. The ITSEC Cybersecurity Summit 2025 therefore served not just as a forum for dialogue but as a catalyst for partnerships, policy thinking, and industry action.

The event demonstrated ITSEC Asia's ambition to position Indonesia as a trusted digital hub for Southeast Asia. By convening experts, decision-makers, and innovators, the summit sent a strong signal that the country is serious about building a resilient cyber ecosystem. It also showcased how collaboration between government, private sector, and academia can drive solutions that no single entity could achieve alone.

As the three-day summit concluded, participants left with more than just new insights. They carried with them a sense of urgency and shared responsibility. In a world where digital infrastructure underpins economies and societies, cybersecurity is not just a technical challenge but a foundation of trust and stability.

This ITSEC Buzz Special edition captures the spirit of the event and goes further, featuring articles from our sponsors who share their perspectives on the latest cybersecurity trends shaping industries today. Together, these stories provide a broader view of where the digital world is heading and how we can secure it. Enjoy the read, and join us in continuing the conversation toward a safer digital future.

ITSEC CYBERSECURITY SUMMIT 2025
The Largest Critical Infrastructure Cybersecurity Event in Southeast Asia

CSIRT: WHY YOUR ORGANIZATION NEED TO HAVE ONE?

By: H. Fransiskus

Picture this: A bustling airport grinds to a halt. Departure boards go dark, check-in counters freeze, and thousands of travelers find themselves stuck in limbo—all because a single digital system went offline.

This is not a movie plot. It is a real-world disruption. Not a power outage, not sabotage—but a small, overlooked vulnerability in cybersecurity. In this hyperconnected, cyberattack do not come crashing through the front door—they sneak in silently, exploiting weaknesses in systems most people don't even think about. And once inside, they can trigger real-world havoc, grinding critical operations to a standstill.

That's why CSIRT (Computer Security Incident Response Team) is not just bureaucratic acronyms anymore—it is the frontline defender. For any organization that relies on digital systems—and let's face it, that's nearly all of them, having a dedicated cyber response team is not optional. It is critical. And the cost of delaying? Your data, your operations, and your reputation.

What is CSIRT?

When cyberattack hits, the first to answer the call is not your IT guy rebooting the router—it is the CSIRT (Computer Security Incident Response Team). This digital guardian monitors, secures, and responds to cyber incidents with speed and precision. Think of them as the SWAT team of cyberspace. And they're becoming more vital than ever. Indonesia's digital footprint has exploded, with internet users skyrocketing from 88.1 million in 2014 to a whopping 221 million in 2024. That's not just growth—it is transformation. The internet is not a luxury anymore; it is woven into the daily lives, businesses, and communities across the archipelago.

The APJII (Indonesian Internet Service Providers Association) reports a continued upward climb—2.67% growth in just one year (2022–2023). And in terms of user demographics, the split is nearly even: 50.7% male and 49.1% female. Digital connectivity is truly a shared experience. As the nation becomes more connected, its vulnerabilities grow too. That's why CSIRT is not just a technical asset—it is a strategic necessity.

From scrolling TikTok to running digital businesses, Indonesia's internet users span nearly every generation—but Gen Z leads the charge. Born between 1997 and 2012, they account for 34.40%

of the nation's online population. Millennials are not far behind at 30.62%, followed by Generation X at 18.98%. Even the Post-Gen Z crowd—those born after 2023—are already online at 9.17%, proving that tech fluency is starting far earlier. Meanwhile, Baby Boomers (6.58%) and Pre-Boomers (just 0.24%) are dipping into digital waters too, though with more caution than click speed.

But here's the catch: despite being hyperconnected, cybersecurity awareness remains low across the board. Many users still lack the basic knowledge, hands-on experience, and technical skills to defend themselves online. And in a landscape this complex, awareness alone won't cut it. Cybersecurity is not just about firewalls or antivirus—it is a strategic collaboration between people, processes, and technology. These three pillars must work in sync to build true digital resilience. Without all three, vulnerabilities linger—and attackers don't wait for anyone to catch up.

People

When it comes to cybersecurity, humans are both the first line of defense—and the biggest vulnerability. No matter how sophisticated the technology or how well-structured the processes are, they're only as effective as the people behind them.

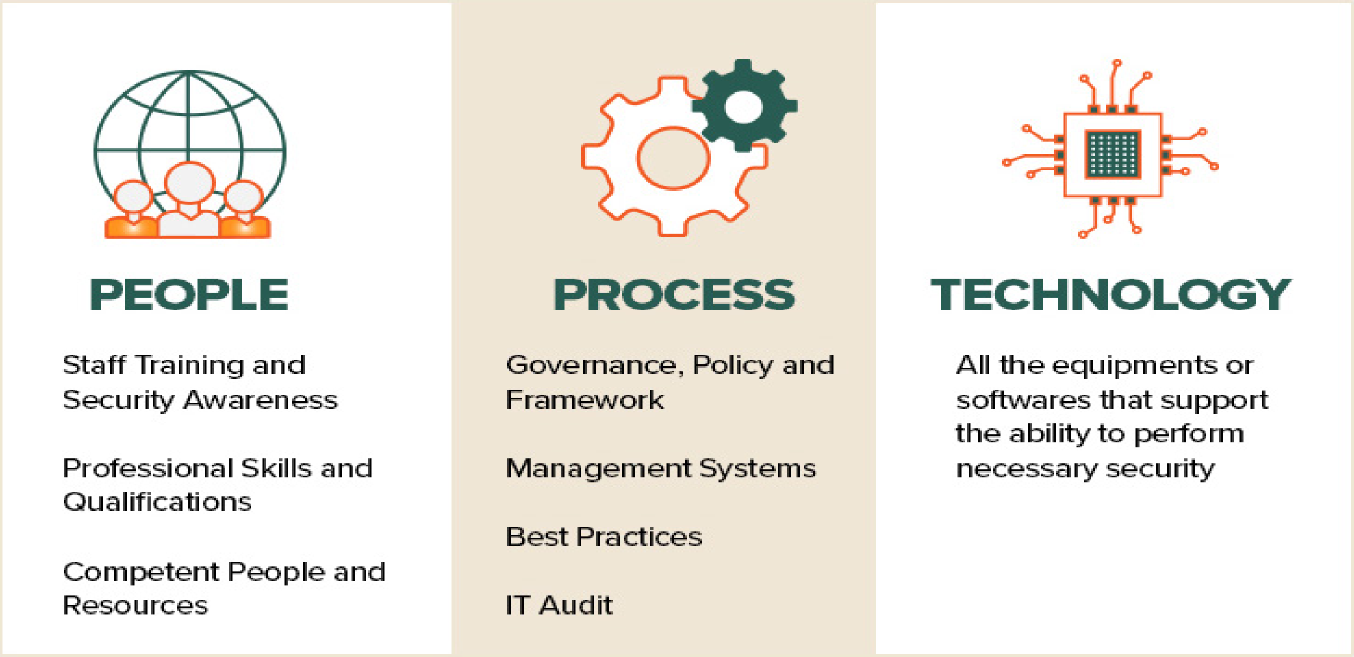
Cybercriminals aren't just code wizards—they're master manipulators of human error. They exploit everyday habits: weak passwords, never changing login credentials, blindly clicking on unfamiliar links. These slip-ups can hand over access to sensitive information without a single line of code breached. Strong cybersecurity doesn't just live in servers and firewalls—it lives in behavior. Which means education, awareness, and vigilance are every bit as critical as technical tools.

Process

Cyberattacks aren't just a threat—they're a test of how well-prepared your organization really is. Having strong technology helps, but without a solid process, even the best tools fall short. Organizations need a clear, step-by-step framework that guides them through every phase of a cyber incident: identify, detect, protect, respond, and recover. This system must be proactive, not reactive, and flexible enough to handle threats from both internal mishaps and external intrusions.

Technology

Tech is the armor, but it needs to cover every point of vulnerability. That means securing three critical layers: endpoint devices (like laptops, smart gadgets, and routers), networks, and the cloud. Tools like firewalls, DNS filters, malware blockers, antivirus software, and email security systems form the digital shield—but they only work if deployed wisely.



PEOPLE

Staff Training and Security Awareness

Professional Skills and Qualifications

Competent People and Resources

PROCESS

Governance, Policy and Framework

Management Systems

Best Practices

IT Audit

TECHNOLOGY

All the equipments or softwares that support the ability to perform necessary security

And even the strongest tech stack needs human oversight. As internet usage grows and attack surfaces widen, organizations must have a dedicated squad on alert: a CSIRT team. They're the rapid-response unit tasked with monitoring systems, containing threats, restoring damage, and documenting every incident for management.

> *Cybersecurity triad: People detect and respond, processes guide actions, and technology enforces security at scale.*

Key Aspects of CSIRT

Think of the Computer Security Incident Response Team (CSIRT) as a high-functioning emergency unit for cyber crises. It's not one-size-fits-all; it's a team with specialized roles that work together to protect digital infrastructure from threats, recover quickly, and prevent future chaos.

Here's how this digital task force operates when trouble strikes:

Incident Mitigation
Once a threat is confirmed, it's action time. The team moves fast—isolating affected systems, removing malicious software, and plugging vulnerabilities before things spiral.

System Recovery
With the threat contained, the focus shifts to restoring normalcy. Damaged systems and lost data are brought back online, ensuring business continues with minimal disruption.

Investigation & Analysis
Every incident is a learning opportunity. CSIRT traces the roots of the breach, analyzes how it happened, and identifies weaknesses—so future attacks don't get the same chance.

Reporting
Finally, all findings are documented in a clear, comprehensive report for management and key stakeholders. This isn't just paperwork—it's the blueprint for smarter defense moving forward.

Behind the scenes, each division of a CSIRT brings deep expertise to the table—from forensic analysis to malware response, turning what could be chaos into coordinated control.

Inside the CSIRT

CSIRT isn't just a label—it's a fully functioning digital response unit. Think of it as a cybersecurity orchestra, where each division plays a distinct instrument, yet harmonizes to respond to incidents with precision and speed. Here's the lineup:

Monitoring & Detection Division
The eyes and ears of the team. This division keeps watch 24/7, scanning logs, analyzing network traffic, and monitoring device activity to spot threats like malware or hacking attempts before they strike.

Incident Response & Mitigation Division
The emergency responders. When an attack hits, this team jumps into action—isolating infected systems, securing critical evidence (from firewalls to forensic snapshots), and patching vulnerabilities so the threat doesn't spread.

Digital Forensics Division
The investigators. They dig deep to uncover the how, when, and why of every incident—analyzing attack footprints and timelines to prevent repeat offenses. Many team members hold advanced forensic certifications and support legal or compliance efforts

Communication & Coordination Division
The bridge-builders. Cyber incidents don't happen in a vacuum, and this division keeps internal teams, leadership, vendors, and even government agencies in sync—whether it's issuing updates or managing external disclosures.

Recovery & Remediation Division
The fixers. After the storm passes, this crew gets systems back on track—restoring data, reconfiguring software, and plugging any lingering security gaps to prevent future breaches.

Types of CSIRT

Beyond the core responsibilities of a CSIRT, it's equally important to recognize the distinct types of teams that operate across different scopes and sectors. Each plays a strategic role in managing cybersecurity incidents tailored to their domain.

Internal CSIRT
Established within an organization, this team is dedicated to respond to incidents affecting internal systems, data, and operations. Think company-exclusive defense unit.

External CSIRT
The reinforcements. These teams are formed by third parties—like security service providers or government agencies—to help organizations respond when internal resources need backup.

Sectoral CSIRT
The specialists. Focused on securing specific industries like banking, healthcare, or energy. They understand the unique risks and regulations in their sector, and tailor their response accordingly.

National CSIRT
Operating at the national level, these teams coordinate responses to cyber incidents that impact broader public infrastructure, critical systems, or pose nationwide threats. They also play a key role in public alerting and inter-agency collaboration.

Why Organization Must Prioritize CSIRT

As Indonesia accelerates toward a more digitized future—with public data stored online and critical sectors like defense, banking, and infrastructure tethered to the internet—the need for a dedicated CSIRT/TTIS team within every organization has become urgent, not optional. Without a proactive cybersecurity response team in place, these organizations face serious exposure. In high-stakes sectors, the consequences of an attack aren't just financial—they're national. In the defense arena, for example, sensitive state intelligence could fall into the wrong hands, threatening public trust and national security.

We've already seen the risks play out. During the ransomware attack on Indonesia's PDN (National Data Center), attackers locked critical systems, cutting off access to essential data for several ministries—including immigration records. The result? Massive airport disruptions, stranded passengers, and operational paralysis that rippled across sectors. Digital vulnerability is no longer hypothetical. It's a strategic weakness that attackers are ready to exploit—and CSIRT/TTIS is the firewall of accountability, speed, and resilience that organizations must build today to avoid crisis tomorrow.

But PDN's ransomware fallout didn't just cripple immigration systems. It echoed across multiple agencies, spotlighting the absence of a systematic cyber preparedness framework. Rather than placing blame on any single entity, the incident forces a broader, more vital question: How prepared are we—truly—to handle such threats? The prolonged recovery process exposed serious gaps, and it's likely many other breaches have yet to be made public. Despite growing awareness, there's still no definitive data on how many Indonesian organizations have a CSIRT team in place. While medium to large institutions are gradually catching on, many are still reactive—taking action only after an incident unfolds

The misconception that "no incident means no risk" lulls organizations into complacency, overlooking the fact that silent vulnerabilities are often the most dangerous. Establishing a CSIRT isn't just a technical upgrade—it's a strategic safeguard. Yes, the setup requires time, talent, and investment. But the cost of inaction? Far greater.

> *In the cybersecurity equation, preparedness isn't a luxury—it's a necessity.*

Personal Data Protection Law

In Indonesia, data protection is no longer just a best practice—it's a legal mandate. Under Law Number 27 of 2022 on Personal Data Protection (PDP), every organization that manages public data is required to uphold strong cybersecurity standards. The goal? Prevent digital incidents that could harm individuals and institutions alike.

Chapter VI (Articles 19–54) clearly outlines the duties of personal data controllers and processors when handling sensitive information. These responsibilities aren't just guidelines—they're enforceable obligations. Chapter VIII, Article 57, lays out administrative sanctions for those who fall short of compliance.

But the stakes go beyond penalties. An organization's reputation is tightly linked to public trust. A single breach—especially one resulting from negligence—can trigger more than technical fallout; it can erode confidence, invite scrutiny, and damage credibility in the eyes of stakeholders.

That's where CSIRTs come in. By monitoring systems, investigating anomalies, and coordinating incident responses, the team helps organizations meet legal duties outlined in Chapter VI, such as ensuring the integrity, confidentiality, and lawful processing of personal data.

Believe it or not,
breaking into system today often requires
no complex exploits at all.

STEALER LOGS UNMASKED: ATTACK, DEFENSE AND THE AUTOMATION EDGE OF BRON VAULT

By: YoKo Kho

Despite years of headlines and hacker movie stereotypes, hacking is still commonly associated with techniques like SQL injection, code execution, privilege escalation, and other attacks that sound sophisticated and hard to pull off.

But in reality, many breaches begin far more simply. No exploits. No fancy payloads. No need to break in. The attacker just walks through the front door with stolen credentials.

And this isn't just an anecdote, it's backed by data. The 2025 Verizon Data Breach Investigations Report (DBIR) found that 32% of all breaches involved stolen credentials.

Where These Credentials Come From?

Technically, they're the product of a well-oiled underground economy where data is systematically harvested, traded, and reused. In recent years, the primary engine of this ecosystem has been stealer malware: a lightweight, evasive program designed to silently extract browser-stored passwords, session cookies, crypto wallets, and other sensitive data from infected machines.

This vast collection of harvested credentials then becomes a valuable commodity for threat actors to trade and exploit. But its impact goes far beyond simple account takeovers. For cybercriminals, it often serves as the gateway for more destructive attacks like ransomware. In fact, the same Verizon report shows that 54% of ransomware victim domains also appeared in stealer logs, underscoring how stealer malware often lays the groundwork for broader compromises.

This connection to ransomware underscores the urgency of understanding just how widespread this problem really is.in place. While medium to large institutions are gradually catching on, many are still reactive—taking action only after an incident unfolds

The Global Battlefield of Stealer Malware

On a global scale, what began as a quiet trend has grown into a full-scale epidemic. Fueled by stealer malware, an underground network of trade has spread across continents, infecting devices in waves and silently harvesting sensitive data from unsuspecting victims.

To grasp the true scale of this silent crisis, we analyzed tens of thousands of stealer malware incidents recorded between January and June 2025. The numbers aren't spread out evenly. Some countries are seeing far more infections than others, pointing to how exposure and risk can vary widely across regions.

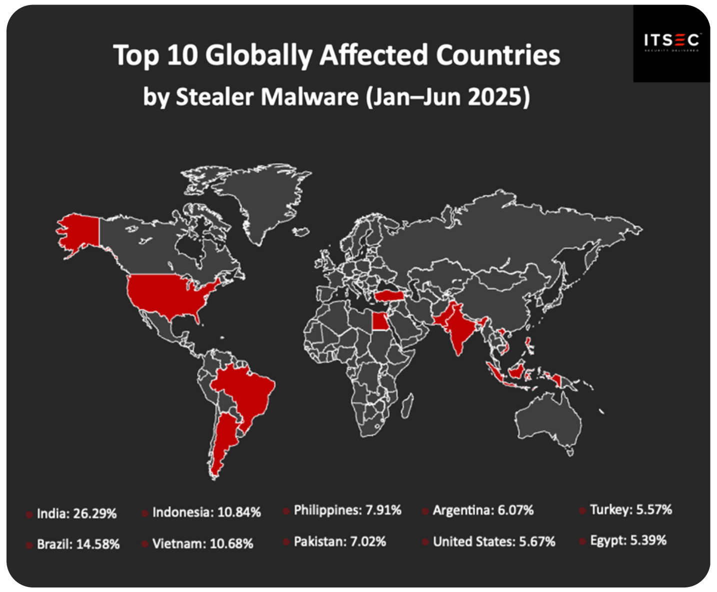


Figure 1: Top 10 Globally Affected Countries (Jan-June 2025)

From a global perspective, we can see that several Asian countries feature prominently among the most affected. While it's too early to draw definitive conclusions about regional risk, the presence of five Asian nations in the top ten collectively accounting for over 60% of observed cases, suggests that the region is facing disproportionately high levels of exposure to stealer malware.

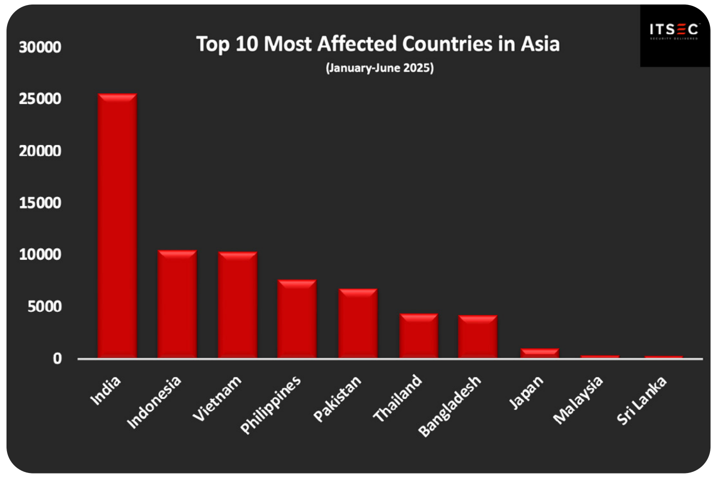


Figure 2: Top 10 Most Affected Asian Countries (Jan-June 2025)

If we look at the Asia region, the infection landscape reveals an even more concentrated pattern. India alone accounts for more than a third (35.70%) of all stealer malware incidents in the region. Following closely behind are Indonesia (14.72%) and Vietnam (14.50%), with the Philippines and Pakistan also contributing significantly.

With infection numbers this high, the real question isn't just about scale, it's about substance. What exactly is being taken, and how? To get a clearer picture of the impact, we need to look beyond the percentages and examine the harvested data from these attacks: stealer logs, which consist of bundles of stolen credentials, session cookies, and other sensitive data.

Anatomy of a Stealer Operation

What is Stealer Log?
When a device is successfully compromised by stealer malware, what actually gets stolen? The answer often lies in the stealer log. This "log" isn't just a single stolen password, it's a curated snapshot of a victim's digital life, neatly organized and either published for free or sold on the underground market.

What makes stealer logs particularly dangerous is how complete and convenient they are. Instead of wading through raw dumps or scattered credentials, threat actors receive a curated bundle: browser-saved passwords, session cookies, autofill entries, and configuration files from apps like VPN clients, password managers, or crypto wallets. Many are tagged with machine and location identifiers, then neatly organized into folders named after the compromised device.

For attackers, it is turnkey access. And for defenders, it is a "forensic" snapshot that offers a view of what the attacker likely saw, touched, and potentially used.
How is Stealer Log Created?
A stealer log doesn't appear out of thin air. It begins with the successful execution of stealer malware on a device, often triggered by the victim themselves.
In many cases, the infection begins with risky behavior such as downloading cracked software, using cheats for online games, running fake installers, or interacting with explicit or gambling content. These are common delivery channels, where the stealer is bundled with a legitimate-looking file or hidden behind an enticing download button. Once the file is executed, the stealer runs silently in the background.

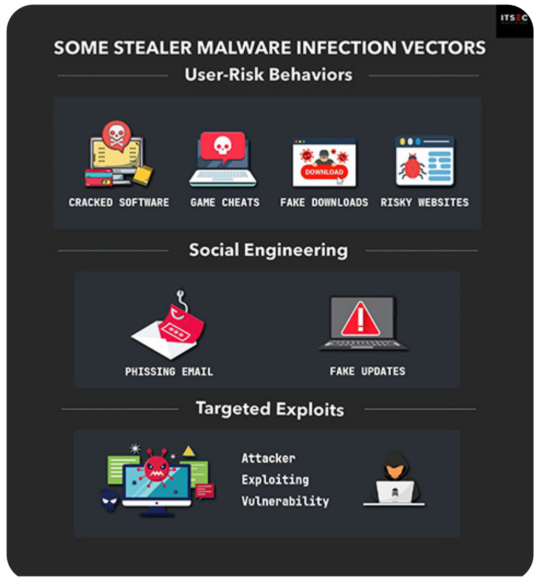


Figure 3: Some Stealer Malware Infection Vectors

However, not all infections rely on user intent. Social engineering tactics such as phishing emails or fake updates delivered through compromised websites are also widely used. In more targeted scenarios, attackers may exploit system vulnerabilities or weak credentials to gain access and deploy the stealer manually, without requiring any user interaction.

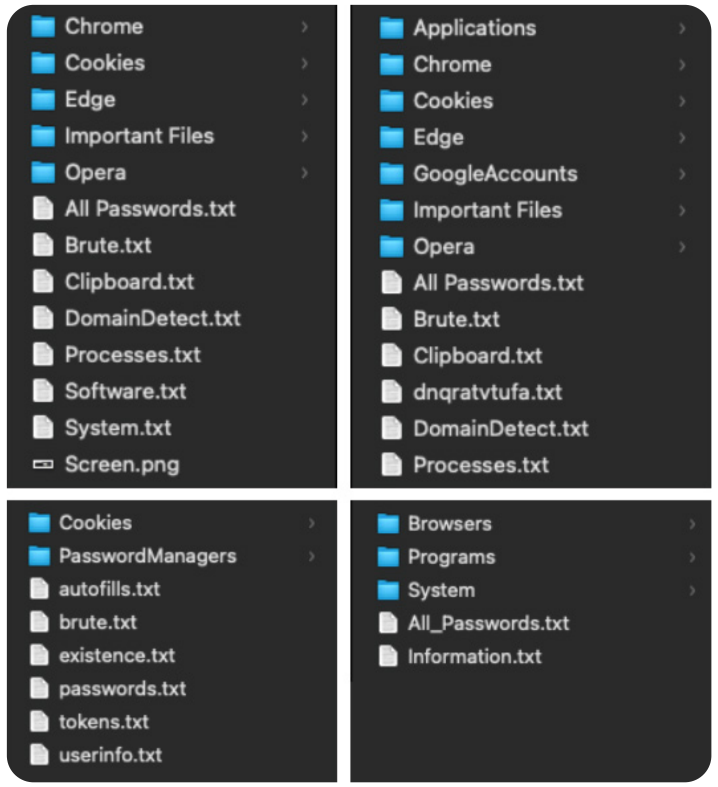
Regardless of the infection method, once the malware is active, it immediately begins the harvesting process. It scans specific file paths, browser databases, and application folders to collect a wide range of sensitive data. This data is typically compressed into a structured archive and may be encrypted before being sent to the attacker's control host or uploaded to a file hosting service.

From infection to exfiltration, the process often takes less than a minute. And when it's done, there's usually no visible trace for the victim. Just a neatly packaged log, now circulating in the underground economy.

What Does Log Typically Contain?
As mentioned, a stealer log is a collection of digital information, structured for optimum efficiency. While capabilities vary between malware families, most logs contain a core set of data harvested from the most common sources on a device.

Chief among these sources is the web browser, a central hub for digital identity. Stealer malware systematically extracts a broad range of sensitive data, including saved usernames and passwords, complete browsing history, session cookies that may, in some cases, allow access to authenticated services, and autofill records that often contain full names, physical addresses, and payment card details.

But the harvesting doesn't stop at the browser. The stealer typically expands its reach by conducting a reconnaissance of the device itself, aiming to build a comprehensive victim profile. It compiles a detailed "system fingerprint," which includes general device and user information like the computer name, hardware ID, OS version, installed software, IP address, and geographical location.



```
Chrome
Cookies
Edge
Important Files
Opera
All Passwords.txt
Brute.txt
Clipboard.txt
DomainDetect.txt
Processes.txt
Software.txt
System.txt
Screen.png
```

```
Applications
Chrome
Cookies
Edge
GoogleAccounts
Important Files
Opera
All Passwords.txt
Brute.txt
Clipboard.txt
dnqratvtufa.txt
DomainDetect.txt
Processes.txt
```

```
Cookies
PasswordManagers
autofills.txt
brute.txt
existence.txt
passwords.txt
tokens.txt
userinfo.txt
```

```
Browsers
Programs
System
All_Passwords.txt
Information.txt
```

Figure 4: Common File Structure Found in Stealer Logs

While this reconnaissance provides valuable context, the capabilities of many modern stealers extend far beyond it. Many stealers are built to pursue even more valuable targets, namely specific applications that hold the keys to a user's digital assets or corporate access. These are not random grabs, they are targeted hunts for data stored in high-value applications used for authentication, remote connectivity, or financial management. The primary targets include:

- Credential vaults from Password Managers, FTP Clients config file, and Email Clients data.
- VPN session tokens and configs used to mimic corporate access.
- Local Crypto Wallet files, such as wallet.dat, and exposed private keys that enable direct asset theft.

The Heart of The Log

From this vast collection of stolen data, one file consistently stands out as the crown jewel in nearly every stealer log: passwords.txt. This file, often named passwords.txt, all-passwords.txt, or a similar variant, is arguably the single most valuable artifact for both attackers and defenders.

What makes it fundamental isn't just its content, but its structured, immediately usable format. Unlike cookies or system files that may require further interpretation, passwords.txt delivers the most sought-after raw data in a clear layout:

- The originating URL or domain.
- The username.
- The password itself.
- The application or browser where the credential was stored .

This "ready-to-use" nature makes passwords.txt the most efficient starting point for analysis. Its presence and quality often serve as the primary factors for an analyst to determine whether a log is high-value or not.

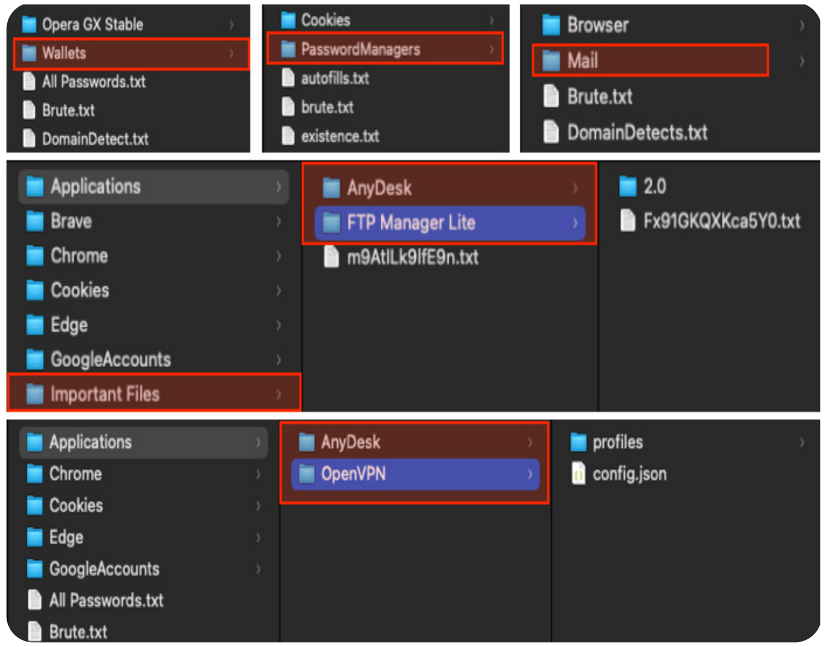
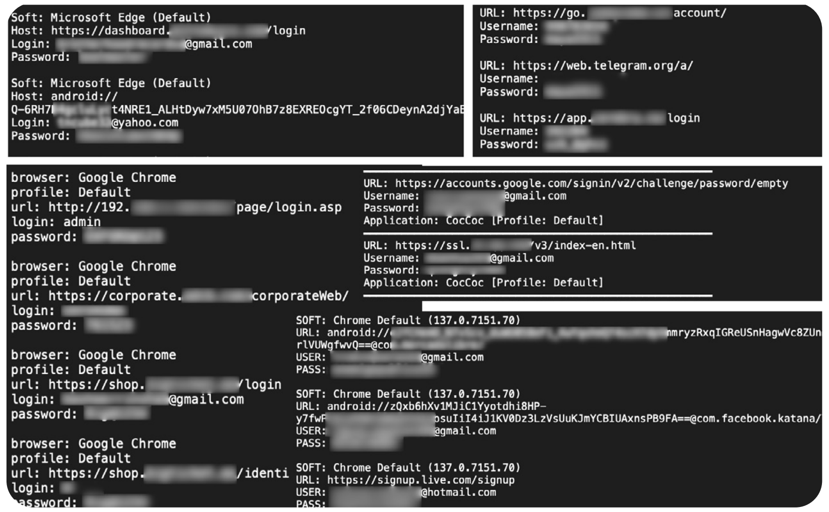


Figure 5: Targeted Data Harvesting by Stealer Malware

Field	Aliases	Description
URL	Host, Hostname, Url	Contains the full web address, including specific paths or endpoints, that the user accessed.
Application	browser, SOFT, Storage	Identifies the source application or browser (e.g., Chrome, Edge) from which the data was exfiltrated.
Username	login, USER	The captured username associated with the corresponding URL.
Password	PASS, password	The captured plain-text password corresponding to the username and URL.

Table 1: Common Stealer Log Fields



```
Soft: Microsoft Edge (Default)
Host: https://dashboard.[redacted]/login
Login: [redacted]@gmail.com
Password: [redacted]

Soft: Microsoft Edge (Default)
Host: android://
Q-6RH7[redacted]t4NRE1_ALHtDyw7xM5U07OhB7z8EXREOcgYT_2f06CDeynA2djYaE
Login: [redacted]@yahoo.com
Password: [redacted]
```

```
URL: https://go.[redacted]account/
Username: [redacted]
Password: [redacted]

URL: https://web.telegram.org/a/
Username:
Password: [redacted]

URL: https://app.[redacted]login
Username: [redacted]
Password: [redacted]
```

```
browser: Google Chrome
profile: Default
url: http://192.[redacted]page/login.asp
login: admin
password: [redacted]

browser: Google Chrome
profile: Default
url: https://corporate.[redacted]corporateWeb/
login: [redacted]
password: [redacted]

browser: Google Chrome
profile: Default
url: https://shop.[redacted]/login
login: [redacted]@gmail.com
password: [redacted]

browser: Google Chrome
profile: Default
url: https://shop.[redacted]/identi
login: [redacted]
password: [redacted]
```

```
URL: https://accounts.google.com/signin/v2/challenge/password/empty
Username: [redacted]@gmail.com
Password: [redacted]
Application: CocCoc [Profile: Default]
──────────────────────────────────────────
URL: https://ssl.[redacted]/v3/index-en.html
Username: [redacted]@gmail.com
Password: [redacted]
Application: CocCoc [Profile: Default]
```

```
SOFT: Chrome Default (137.0.7151.70)
URL: android://[redacted]mmryzRxqIGReUSnHagwVc8ZUn
rlVUWgfwvQ==@co[redacted]
USER: [redacted]@gmail.com
PASS: [redacted]

SOFT: Chrome Default (137.0.7151.70)
URL: android://zQxb6hXv1MJiC1Yyotdhi8HP-
y7fwP[redacted]osuIiI4iJ1KV0Dz3LzVsUuKJmYCBIUAxnsPB9FA==@com.facebook.katana/
USER: [redacted]@gmail.com
PASS: [redacted]

SOFT: Chrome Default (137.0.7151.70)
URL: https://signup.live.com/signup
USER: [redacted]@hotmail.com
PASS: [redacted]
```

Figure 6: Content of the Password File

Ultimately, this file itself is the 'stolen key' that enables a new class of attacks.

This new reality, where attackers can often bypass the hunt for vulnerabilities entirely by simply using stolen keys, has profound implications for how we approach security.

This raises a critical question, "***If attackers have such a powerful tool at their disposal, how can security professionals, on both the offensive and defensive sides, leverage this same "attacker's-eye view" for their own purposes?***"

The answer lies in understanding the practical applications of these logs in modern security testing and incident response.

If attackers have such a powerful tool at their disposal, how can security professionals, on both the offensive and defensive sides, leverage this same "attacker's-eye view" for their own purposes?

Leveraging Stealer Logs for Attack and Defense

The existence of stealer logs has reshaped not only how attacks unfold but also how security professionals can anticipate, replicate, and defend against them. These logs offer more than just a list of stolen assets, they provide a rare glimpse into how attackers operate, and more importantly, what they now expect to find.

From an offensive perspective, stealer logs have quietly become an unconventional shortcut into hardened environments. In scenarios where the front door remains locked, where login pages are reduced to minimal functionality, and brute-force entry seems futile, data from a stealer log can serve as a skeleton key, granting access not just to accounts, but to deeper layers of the system, often bypassing traditional exploitation entirely.

On the other hand, for defenders, the appearance of a stealer log should ring louder alarm bells than most common alerts. It doesn't just indicate a potential compromise, it suggests an actual exfiltration has already occurred, and the attacker may have interacted with or replicated an active login using stolen session data. Recognizing this requires defenders to move beyond just cleaning the infected endpoint, it demands a forensic mindset and a re-evaluation of trust across affected systems.

So in this chapter, we will explore how both offensive operators and defenders are beginning to adapt to this stealer-fueled reality, and why understanding these logs may become essential for both attack simulation and incident response.

Stealer Logs in Offensive Ops: Through The Front Door

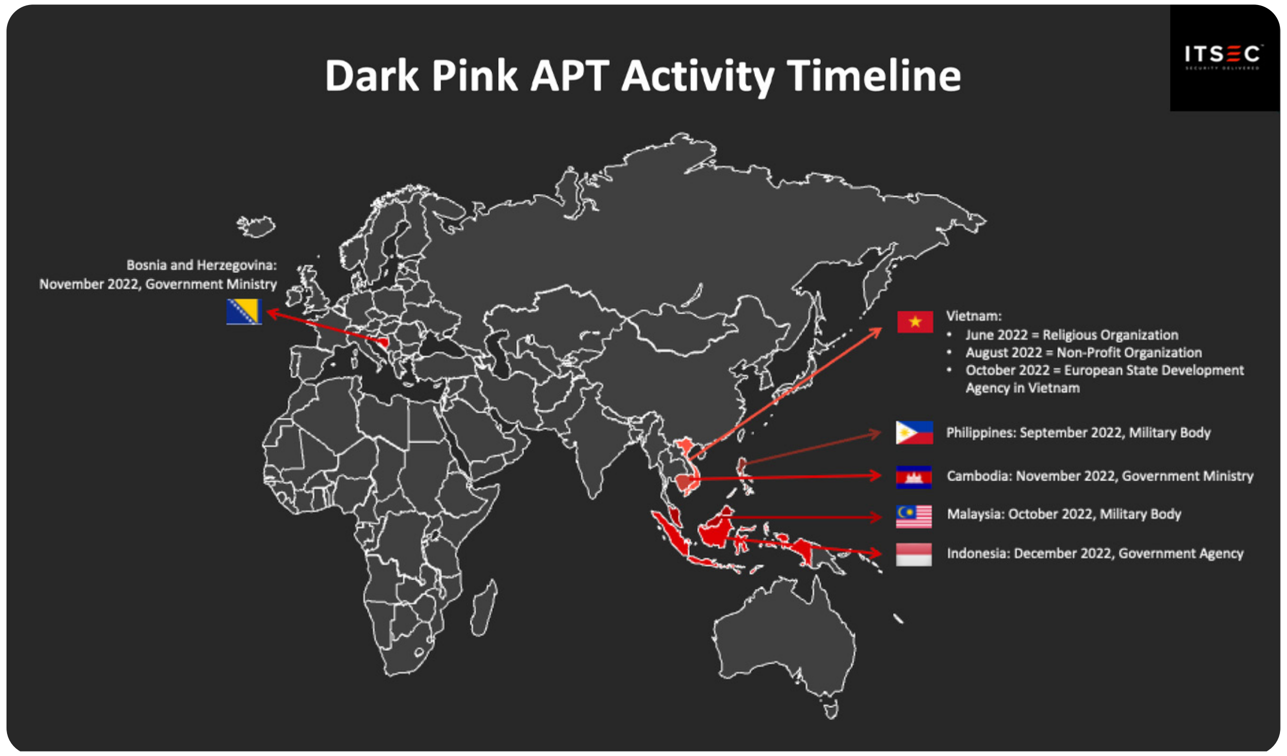
In real-world engagements, we know that not every target is misconfigured or wide open. Many enterprise applications expose only a minimal attack surface, a single login form, no public APIs, no debug paths in sight. These are what we often refer to as "hardened fronts," where the initial stages of testing become a familiar cycle of dead ends. Hours are spent crawling for endpoints, brute-forcing logins, and injecting every imaginable parameter, all yielding no results. Even deep reconnaissance across collaboration tools like GitHub or Atlassian can come up empty.

This repeated failure often forces a shift in strategy. At some point, rather than pushing harder, we can start looking for the doorkey hidden somewhere else entirely, often found in stealer logs.

This shift in mindset mirrors the operational reality of many advanced threat groups. Take, for example, the APT group Dark Pink. As documented in industry reports, their operations targeting government and military entities across Southeast Asia, including Indonesia, Malaysia, and the Philippines, often begin not with exploiting a software vulnerability, but with carefully crafted spear-phishing emails designed to capture login credentials. By luring victims into entering their passwords on fake portals, Dark Pink gains the "keys to the kingdom" without ever breaching a single line of code.

While their credential theft technique differs from stealer malware, the principle is the same, valid credentials unlock more than just access. The difference is that stealer logs scale this tactic passively, collecting credentials in bulk as victims unknowingly execute malicious loaders or cracked software bundled with stealer malware.

But how does this threat play out in day-to-day corporate environments and offensive engagements? The principles remain the same, but the opportunities often arise from more common, everyday situations.



Dark Pink APT Activity Timeline

Bosnia and Herzegovina:
November 2022, Government Ministry

Vietnam:
- June 2022 = Religious Organization
- August 2022 = Non-Profit Organization
- October 2022 = European State Development Agency in Vietnam

Philippines: September 2022, Military Body

Cambodia: November 2022, Government Ministry

Malaysia: October 2022, Military Body

Indonesia: December 2022, Government Agency

Figure 7: Dark Pink APT Activity Timeline

Field Note I

The Leaky Browser Profile

In one real-world investigation, we encountered an employee who had synced their corporate browser profile on a shared home PC, used by their spouse and children. While gaming, the child installed cheat tools laced with stealer malware. This led to the compromise of not just the child's credentials, but also the parent's, including their corporate SSO account.

What began as a child downloading a game cheat on a family computer had now escalated into a direct threat to the corporate network, all due to a single, leaky browser profile.

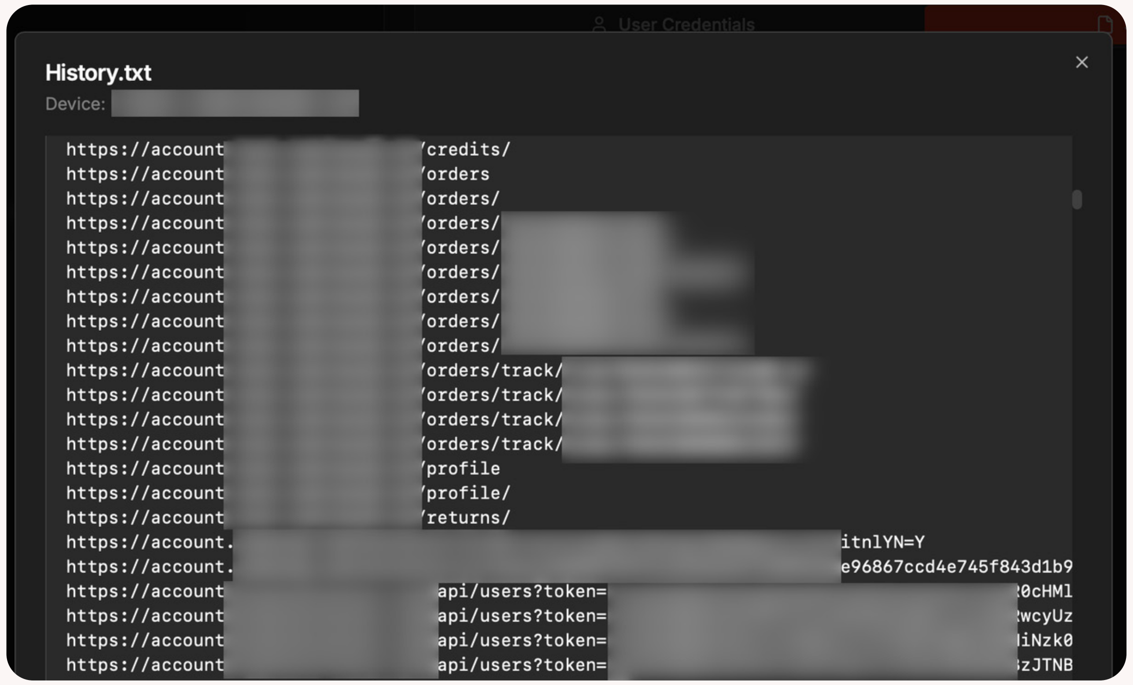
This case perfectly illustrates how the modern attack surface reaches deep into personal territory, and why the corporate security boundary no longer stops at the office firewall. The real weakness wasn't in the code, but in a policy that let a trusted identity bleed into an untrusted environment. For an attacker, exploiting these kinds of policy gaps and human behaviors is often far more effective than searching for a traditional software flaw.

Field Note II

How Stealer Logs Turned UUID-Based Access Control into a Flaw

In another case, we discovered a broken access control issue where user data was protected solely by UUIDs embedded in the URL. However, this created a classic dilemma: while the vulnerability clearly existed, it seemed practically unexploitable since UUIDs are random, non-sequential, and hard to guess.

However, that changed. When we analyzed a large set of stealer logs, we found multiple victims who had used this application. By reviewing their URL history, we harvested a substantial number of valid UUIDs, effectively turning a theoretical issue into a working exploit path. No passwords, no session hijacking. Just raw URLs leading straight to private data.



History.txt

Device: [redacted]

```
https://account[redacted]/credits/
https://account[redacted]/orders
https://account[redacted]/orders/
https://account[redacted]/orders/[redacted]
https://account[redacted]/orders/[redacted]
https://account[redacted]/orders/[redacted]
https://account[redacted]/orders/[redacted]
https://account[redacted]/orders/[redacted]
https://account[redacted]/orders/[redacted]
https://account[redacted]/orders/track/[redacted]
https://account[redacted]/orders/track/[redacted]
https://account[redacted]/orders/track/[redacted]
https://account[redacted]/orders/track/[redacted]
https://account[redacted]/profile
https://account[redacted]/profile/
https://account[redacted]/returns/
https://account.[redacted]itnlYN=Y
https://account.[redacted]e96867ccd4e745f843d1b9
https://account[redacted]api/users?token=[redacted]0cHMl
https://account[redacted]api/users?token=[redacted]wcyUz
https://account[redacted]api/users?token=[redacted]iNzk0
https://account[redacted]api/users?token=[redacted]zJTNB
```

Figure 8: A Substantial Number of UUIDs in Browser History

A reasonable question might be, "If the logs contain passwords, why bother exploiting broken access control?" In some cases, that's a valid point. However, the application in question supported multiple login methods, namely users could either log in with a username and password, or use a passwordless flow by providing their phone number and receiving a one-time code.

In scenarios where the passwordless option was used, credentials stolen by a stealer wouldn't be sufficient to gain access. But a leaked UUID from the victim's browser history still granted direct access to private user data, making broken access control the most effective path for the attacker to access user data.

The Blue Team Perspective

On the defensive side, discovering that credentials or tokens from the environment appear in a stealer log is a high-priority indicator of deeper compromise. Unlike commodity malware alerts, which might be quarantined and forgotten, a stealer log is proof that exfiltration occurred, and possibly that access is being resold or reused.

This reality means that traditional playbooks, which often stop at isolating the endpoint and resetting a password, are no longer sufficient. A broader lens is required, because once credentials are exfiltrated, the attack surface extends far beyond the initial device, potentially enabling access to web portals, internal tools, VPNs, or any third-party services where those same credentials may still be valid.

In practice, adopting this broader lens means asking a new set of forensic questions: Where else were these credentials used? Are the stolen session cookies still valid, potentially allowing attackers to bypass MFA? Has the account been accessed from unknown IPs or geographies? Without these answers, defenders risk overlooking silent, credential-based persistence.

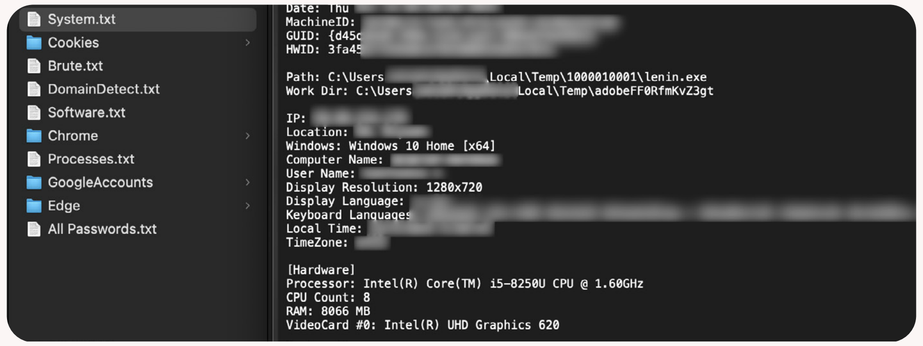
Blue Team Note

Finding the Infection's Fingerprints

As an additional note, beyond the reactive measures of managing the resulting security risks, the stealer log itself can, in certain situations, become a direct source of information for obtaining Indicators of Compromise (IoCs). This involves looking past the stolen credentials and examining the operational artifacts left behind by the malware's execution.

Valuable forensic clues can often be found within bundled files like system.txt or information.txt. Instead of just seeing a list of stolen passwords, a defender might find:

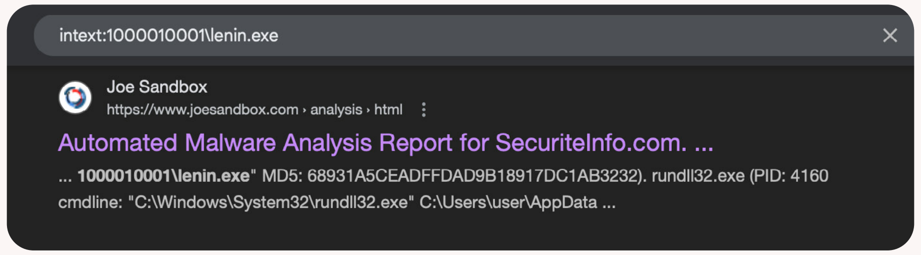
- Suspicious file paths or executable names that point directly to the malware on disk.
- A list of running processes.
- Known malicious domains or C2 server addresses tucked away in browser history files.



```
Date: Thu [redacted]
MachineID: [redacted]
GUID: {d45c[redacted]
HWID: 3fa45[redacted]

Path: C:\Users[redacted]Local\Temp\1000010001\lenin.exe
Work Dir: C:\Users[redacted]Local\Temp\adobeFF0RfmKvZ3gt

IP: [redacted]
Location: [redacted]
Windows: Windows 10 Home [x64]
Computer Name: [redacted]
User Name: [redacted]
Display Resolution: 1280x720
Display Language: [redacted]
Keyboard Languages[redacted]
Local Time: [redacted]
TimeZone: [redacted]

[Hardware]
Processor: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
CPU Count: 8
RAM: 8066 MB
VideoCard #0: Intel(R) UHD Graphics 620
```

Figure 9: Sample of System.txt

With a potential malware name and path in hand, the investigation can begin. A simple search online often immediately links these artifacts to known malware campaigns, as documented by other researchers or automated analysis platforms.



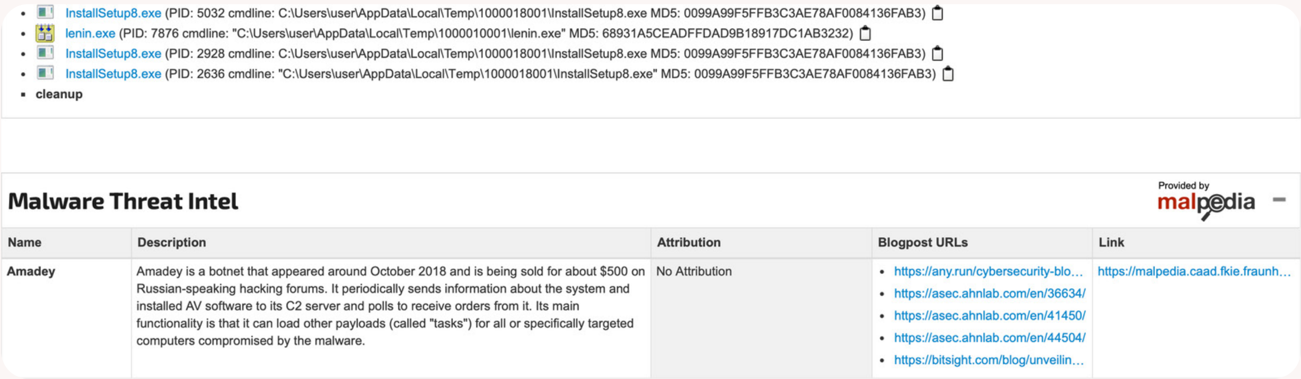
intext:1000010001\lenin.exe

Joe Sandbox
https://www.joesandbox.com › analysis › html

Automated Malware Analysis Report for SecureInfo.com. ...

... **1000010001\lenin.exe**" MD5: 68931A5CEADFFDAD9B18917DC1AB3232). rundll32.exe (PID: 4160 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData ...

Figure 10: Search for Information Using a Search Engine



- InstallSetup8.exe (PID: 5032 cmdline: C:\Users\user\AppData\Local\Temp\1000018001\InstallSetup8.exe MD5: 0099A99F5FFB3C3AE78AF0084136FAB3)
- lenin.exe (PID: 7876 cmdline: "C:\Users\user\AppData\Local\Temp\1000010001\lenin.exe" MD5: 68931A5CEADFFDAD9B18917DC1AB3232)
- InstallSetup8.exe (PID: 2928 cmdline: C:\Users\user\AppData\Local\Temp\1000018001\InstallSetup8.exe MD5: 0099A99F5FFB3C3AE78AF0084136FAB3)
- InstallSetup8.exe (PID: 2636 cmdline: "C:\Users\user\AppData\Local\Temp\1000018001\InstallSetup8.exe" MD5: 0099A99F5FFB3C3AE78AF0084136FAB3)
- **cleanup**

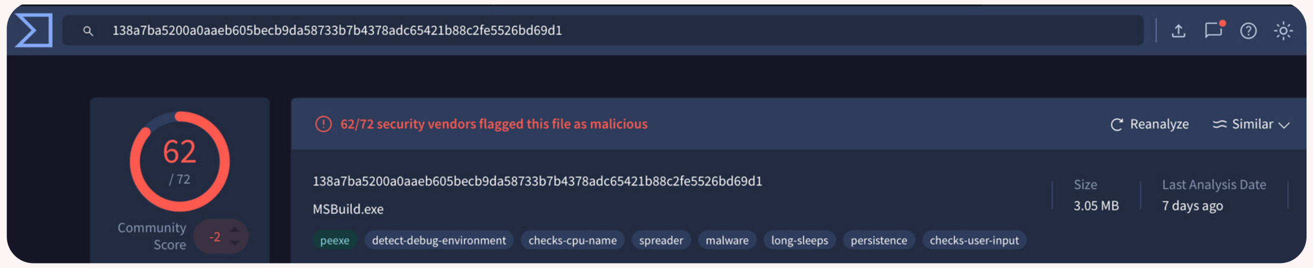
Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Amadey	Amadey is a botnet that appeared around October 2018 and is being sold for about $500 on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads (called "tasks") for all or specifically targeted computers compromised by the malware.	No Attribution	https://any.run/cybersecurity-blo... https://asec.ahnlab.com/en/36634/ https://asec.ahnlab.com/en/41450/ https://asec.ahnlab.com/en/44504/ https://bitsight.com/blog/unveilin...	https://malpedia.caad.fkie.fraunh...

Figure 11: External Intelligence Analysis

The malware's hash can also be checked against VirusTotal to obtain additional insights into how various security vendors classify the file.


138a7ba5200a0aaeb605becb9da58733b7b4378adc65421b88c2fe5526bd69d1
62
/ 72
Community Score
-2
Reanalyze
Similar

62/72 security vendors flagged this file as malicious

138a7ba5200a0aaeb605becb9da58733b7b4378adc65421b88c2fe5526bd69d1

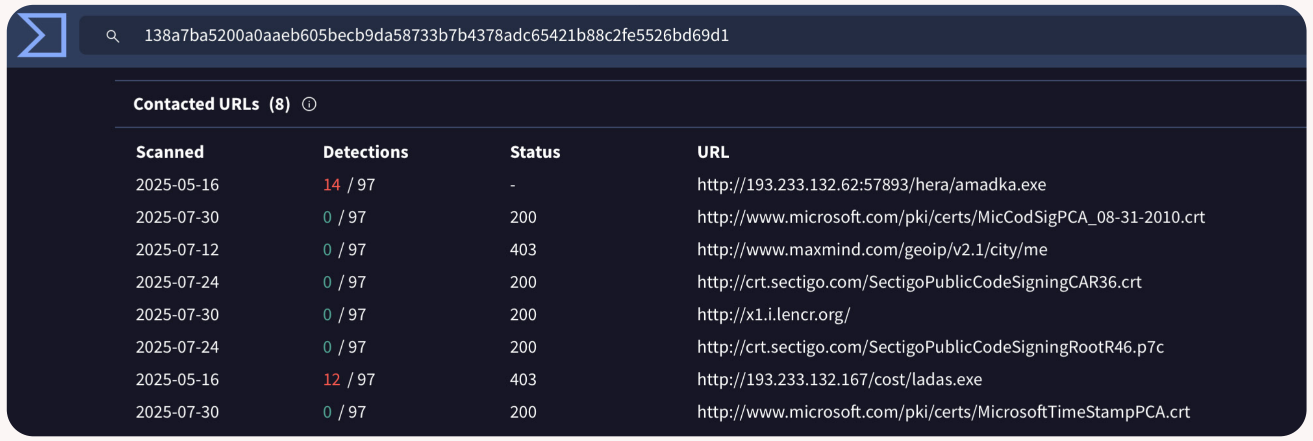
MSBuild.exe

Size: 3.05 MB

Last Analysis Date: 7 days ago

peexe · detect-debug-environment · checks-cpu-name · spreader · malware · long-sleeps · persistence · checks-user-input

Figure 12: Analysis from VirusTotal



138a7ba5200a0aaeb605becb9da58733b7b4378adc65421b88c2fe5526bd69d1

Contacted URLs (8)

Scanned	Detections	Status	URL
2025-05-16	14 / 97	-	http://193.233.132.62:57893/hera/amadka.exe
2025-07-30	0 / 97	200	http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt
2025-07-12	0 / 97	403	http://www.maxmind.com/geoip/v2.1/city/me
2025-07-24	0 / 97	200	http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
2025-07-30	0 / 97	200	http://x1.i.lencr.org/
2025-07-24	0 / 97	200	http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c
2025-05-16	12 / 97	403	http://193.233.132.167/cost/ladas.exe
2025-07-30	0 / 97	200	http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt

Figure 13: Analysis from VirusTotal (2)

Nevertheless, once potential IoCs like file hashes, paths, or domains are validated, they become tangible assets for proactive defense. This intelligence enables security teams to hunt for the specific threat across the company, create robust endpoint detection rules (e.g., YARA), and block the associated malicious infrastructure. In essence, leveraging the log in this manner effectively transforms it from a simple alert about a data leak into a source of high-fidelity intelligence, allowing a holistic response that not only manages the symptom but also helps eradicate the root cause.

A quick note on the method: Unlike traditional digital forensics, which uses structured data from controlled systems, clues gathered from stealer logs are inherently presumptive. They may be outdated or incomplete, so the goal isn't to prove anything conclusively—but to uncover strong leads that guide deeper internal investigations.

By adopting this two-pronged approach, simultaneously tracking the compromised credentials downstream while hunting the source malware upstream, forms the foundation of a mature incident response program. It ensures that for any known compromise, a security team can effectively address both the immediate symptoms and the root cause.

Building on this foundation, defense teams should evolve their approach towards a more proactive strategy. This means they should treat stealer logs not just as records of past compromises, but as a vital source of external threat telemetry, an indicator of what adversaries know and could potentially use.

In practice, this involves systematically ingesting stealer datasets into detection pipelines to be cross-referenced against the internal environment. This includes both mapping exposed credentials to known employees and using discovered malware artifacts (like file hashes and C2 domains) for proactive, enterprise-wide threat hunting. This proactive stance makes it possible to spot and neutralize credential-based intrusions before they escalate, even if they bypass traditional malware defenses.

Equally important is coordination. If the exposed credentials belong to a third-party vendor, then security extends beyond your network. Incident response in these cases may require engaging with partners, rotating shared secrets, and reviewing logs in systems you don't fully control.

Streamlining Stealer Log Analysis

The Analysis Bottleneck: Drowning in Data

The "Leaky Browser Profile" case we explored earlier is a stark reminder of how easily a corporate credential can land in an attacker's hands, all from a single stealer log, triggered by something as trivial as downloading a gaming cheat on a home PC.

Now, imagine facing not just one log, but an entire dump containing data from hundreds of different devices. The challenge immediately shifts from a simple treasure hunt to surviving an avalanche of information.

Faced with this avalanche, an analyst's process becomes a brute-force search for relevance. The typical starting point isn't a specific "device" folder, it's the raw passwords.txt (or similar) files inside each one. The work is a painfully manual grind, open a wall of text, Ctrl+F for keywords like @company-domain.com, vpn, or internal, and repeat across hundreds of folders, each representing a different compromised machine.

It's true that a custom script can be written to scan for specific keywords and pinpoint the exact directory (or "device") containing the target information. And while this certainly speeds up initial filtering, it often stops at surface-level matches. It's a helpful shortcut, but one that still requires an analyst to manually open raw files, leaving the door open for missed context and repetitive effort.

This workflow creates a major capability gap. While large enterprises can absorb this complexity with custom tooling and dedicated teams, the reality for most security professionals, researchers, understaffed SOCs, and smaller businesses is that they are left relying on manual processes that don't scale, putting them at a serious disadvantage in a fast-moving threat landscape.

> *A fair question at this point is "Why not just automate this?"*

Introducing Broń Vault

What if, instead of writing ad-hoc scripts, you could just drag and drop entire .zip files into a simple web-based tool? Imagine a tool that instantly extracts and structures the credentials for quick searching, while still preserving full access to the entire original log: every cookie, system file, and browser artifact, all in one place.

That is the question that led to the creation of **Broń Vault**, an open source stealer logs dashboard.

Broń Vault is our answer to a challenge we see every day in the industry, which is, how to effectively serve the day-to-day needs of security teams on the front lines, who often lack a straightforward alternative to manual scripting or complex platforms. It reflects our core mission at **PT ITSEC Asia Tbk** to democratize security, making foundational capabilities accessible to everyone. Our goal is to eliminate the grunt work of log parsing, so you can focus on what truly matters: making critical security decisions, fast.

> **In line with our mission, Broń Vault is released as a free, open-source project. We invite the community to download and contribute to the tool on our official GitHub repository: https://github.com/itsec-research/bron-vault**

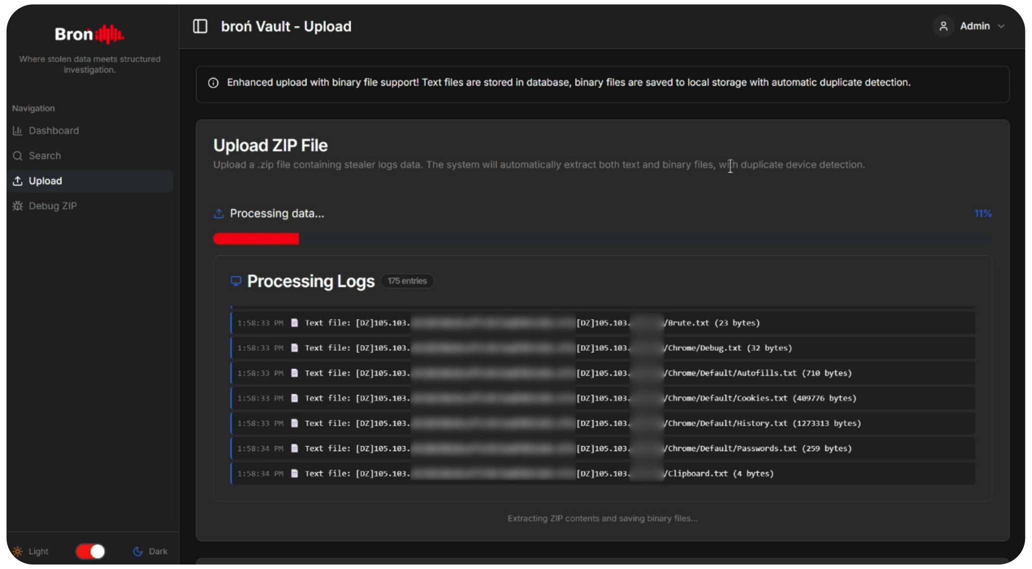
Here is a brief overview of its core features:

1. ***Getting Started: Uploading and Validating Data***

Broń Vault is designed to be as simple as possible. Forget complex setups or command-line gymnastics. You can simply drag and drop your .zip log files directly into the Upload interface. **Broń Vault** handles the rest, automatically parsing and structuring the data in the background, making it immediately available for analysis through the Dashboard and Search modules.

> *But what if we're unsure whether a file follows the structure commonly used by threat actors?"*

For situations where we're dealing with unfamiliar or potentially incomplete archives, we've also included a lightweight Debug-Zip utility. This tool lets us to perform a quick pre-flight check on any .zip file, analyzing its internal structure to see if it matches typical stealer formats. Importantly, it also flags any device directories that are missing a password file (passwords.txt or equivalent), which can often indicate a corrupt or low-value log. It's a fast way to triage incoming files, so you can proceed with confidence and focus on what matters.



Enhanced upload with binary file support! Text files are stored in database, binary files are saved to local storage with automatic duplicate detection.

Upload ZIP File

Upload a .zip file containing stealer logs data. The system will automatically extract both text and binary files, with duplicate device detection.

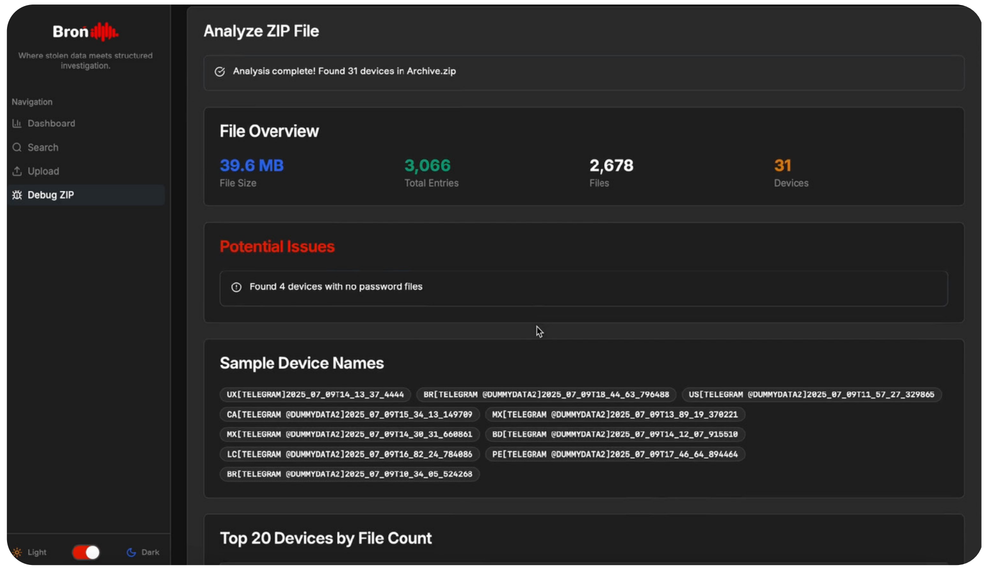
Processing data... 11%

Processing Logs 175 entries

```
1:58:33 PM  Text file: [DZ]105.103.[redacted][DZ]105.103.[redacted]/Brute.txt (23 bytes)
1:58:33 PM  Text file: [DZ]105.103.[redacted][DZ]105.103.[redacted]/Chrome/Debug.txt (32 bytes)
1:58:33 PM  Text file: [DZ]105.103.[redacted][DZ]105.103.[redacted]/Chrome/Default/Autofills.txt (710 bytes)
1:58:33 PM  Text file: [DZ]105.103.[redacted][DZ]105.103.[redacted]/Chrome/Default/Cookies.txt (409776 bytes)
1:58:33 PM  Text file: [DZ]105.103.[redacted][DZ]105.103.[redacted]/Chrome/Default/History.txt (1273313 bytes)
1:58:34 PM  Text file: [DZ]105.103.[redacted][DZ]105.103.[redacted]/Chrome/Default/Passwords.txt (259 bytes)
1:58:34 PM  Text file: [DZ]105.103.[redacted][DZ]105.103.[redacted]/Clipboard.txt (4 bytes)
```

Extracting ZIP contents and saving binary files...

Figure 14: Broń Vault - Upload Feature



Analyze ZIP File

Analysis complete! Found 31 devices in Archive.zip

File Overview

39.6 MB	3,066	2,678	31
File Size	Total Entries	Files	Devices

Potential Issues

Found 4 devices with no password files

Sample Device Names

```
UX[TELEGRAM]2025_07_09T14_13_37_4444   BR[TELEGRAM @DUMMYDATA2]2025_07_09T18_44_63_796488   US[TELEGRAM @DUMMYDATA2]2025_07_09T11_57_27_329865
CA[TELEGRAM @DUMMYDATA2]2025_07_09T15_34_13_149709   MX[TELEGRAM @DUMMYDATA2]2025_07_09T13_89_19_370221
MX[TELEGRAM @DUMMYDATA2]2025_07_09T14_30_31_660861   BD[TELEGRAM @DUMMYDATA2]2025_07_09T14_12_07_915510
LC[TELEGRAM @DUMMYDATA2]2025_07_09T16_82_24_784086   PE[TELEGRAM @DUMMYDATA2]2025_07_09T17_46_64_894464
BR[TELEGRAM @DUMMYDATA2]2025_07_09T10_34_05_524268
```

Top 20 Devices by File Count

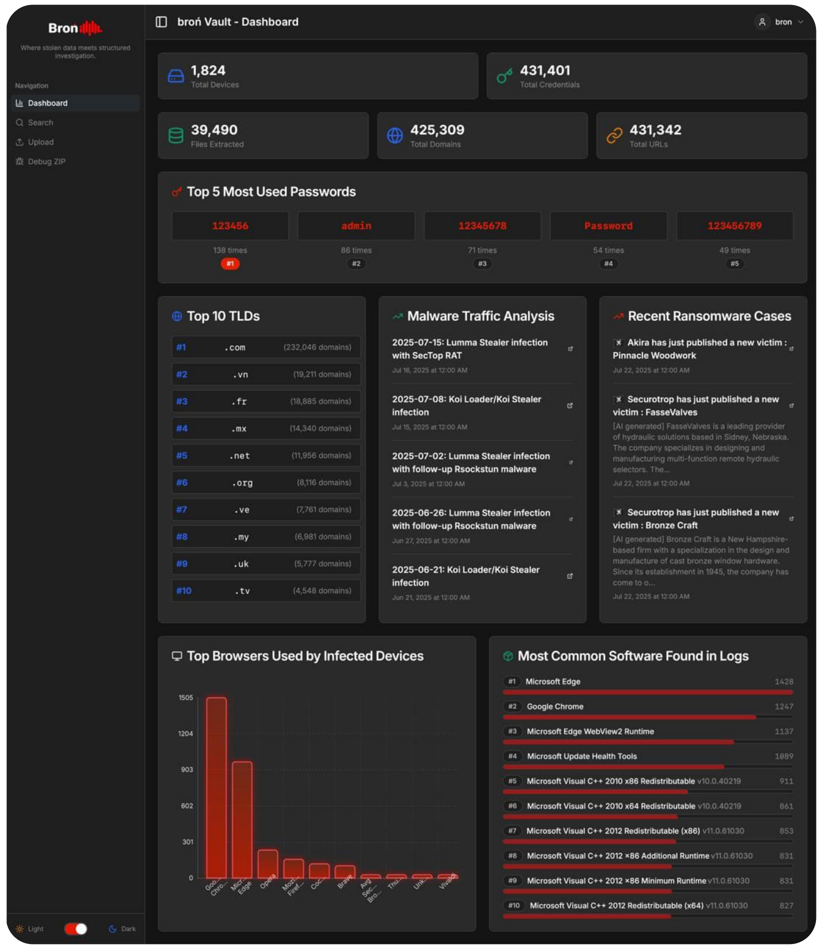
Figure 15: Broń Vault - Debug-Zip Feature

2. ***The 30,000-Foot View (Dashboard)***

Instead of drowning you in a wall of text, Broń Vault immediately presents a high-level Dashboard. This gives you an instant strategic overview of the entire dataset, answering critical questions at a glance: How many devices and credentials are in this dump? What are the most common passwords that could indicate weak patterns? Which top-level domains (.tld) are most affected? What are the most common browsers or software being used, hinting at potential attack vectors?

Under the hood, we've already separated key components typically found in stealer logs, for example, credentials (including TLDs, domains, and browsers stored in distinct fields) and installed software.

Technically, this architecture is extensible by design. For example, correlating infection-time IPs could enable future features like regional threat mapping. In short, Broń Vault is designed not as a static tool, but it is a living, evolving open-source project.



broń Vault - Dashboard

1,824 Total Devices	431,401 Total Credentials	
39,490 Files Extracted	425,309 Total Domains	431,342 Total URLs

Top 5 Most Used Passwords

123456	admin	12345678	Password	123456789
138 times	86 times	71 times	54 times	49 times
#1	#2	#3	#4	#5

Top 10 TLDs

#1	.com	(232,046 domains)
#2	.vn	(19,211 domains)
#3	.fr	(18,885 domains)
#4	.mx	(14,340 domains)
#5	.net	(11,956 domains)
#6	.org	(8,116 domains)
#7	.ve	(7,761 domains)
#8	.my	(6,981 domains)
#9	.uk	(5,777 domains)
#10	.tv	(4,548 domains)

Malware Traffic Analysis

2025-07-15: Lumma Stealer infection with SecTop RAT
Jul 16, 2025 at 12:00 AM

2025-07-08: Koi Loader/Koi Stealer infection
Jul 15, 2025 at 12:00 AM

2025-07-02: Lumma Stealer infection with follow-up Rsockstun malware
Jul 3, 2025 at 12:00 AM

2025-06-26: Lumma Stealer infection with follow-up Rsockstun malware
Jun 27, 2025 at 12:00 AM

2025-06-21: Koi Loader/Koi Stealer infection
Jun 21, 2025 at 12:00 AM

Recent Ransomware Cases

Akira has just published a new victim : Pinnacle Woodwork
Jul 22, 2025 at 12:00 AM

Securotrop has just published a new victim : FasseValves
[AI generated] FasseValves is a leading provider of hydraulic solutions based in Sidney, Nebraska. The company specializes in designing and manufacturing multi-function remote hydraulic selectors. The...
Jul 22, 2025 at 12:00 AM

Securotrop has just published a new victim : Bronze Craft
[AI generated] Bronze Craft is a New Hampshire-based firm with a specialization in the design and manufacture of cast bronze window hardware. Since its establishment in 1945, the company has come to o...
Jul 22, 2025 at 12:00 AM

Top Browsers Used by Infected Devices

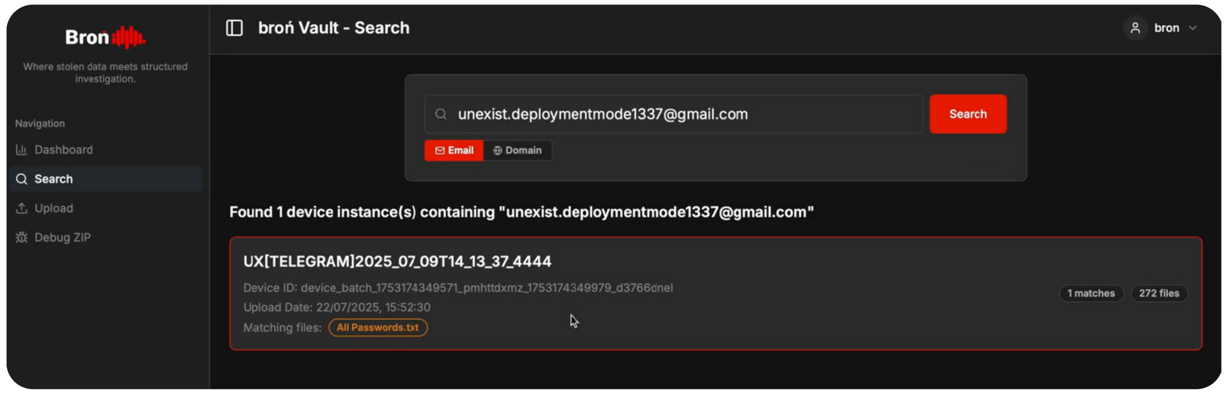
Most Common Software Found in Logs

#1	Microsoft Edge	1428
#2	Google Chrome	1247
#3	Microsoft Edge WebView2 Runtime	1137
#4	Microsoft Update Health Tools	1089
#5	Microsoft Visual C++ 2010 x86 Redistributable v10.0.40219	911
#6	Microsoft Visual C++ 2010 x64 Redistributable v10.0.40219	861
#7	Microsoft Visual C++ 2012 Redistributable (x86) v11.0.61030	853
#8	Microsoft Visual C++ 2012 x86 Additional Runtime v11.0.61030	831
#9	Microsoft Visual C++ 2012 x86 Minimum Runtime v11.0.61030	831
#10	Microsoft Visual C++ 2012 Redistributable (x64) v11.0.61030	827

Figure 16: Broń Vault Dashboard

3. ***Powerful Correlated Search (Search)***
This is the core of Broń Vault. The Search functionality is built to eliminate the nightmare of manual correlation. You can perform lightning-fast lookups by domain (e.g., company-domain.tld) or email, and this is where the real value starts to unfold.

Instead of showing just a plain line of text, a successful match displays the credential along with a tab of correlated data labeled "Supporting Files". This tab reveals all other files stolen from the same device. With a single click, you can pivot from a discovered password to viewing the victim's browser history, inspecting stolen cookies, or exploring other extracted files, all without ever leaving the interface.



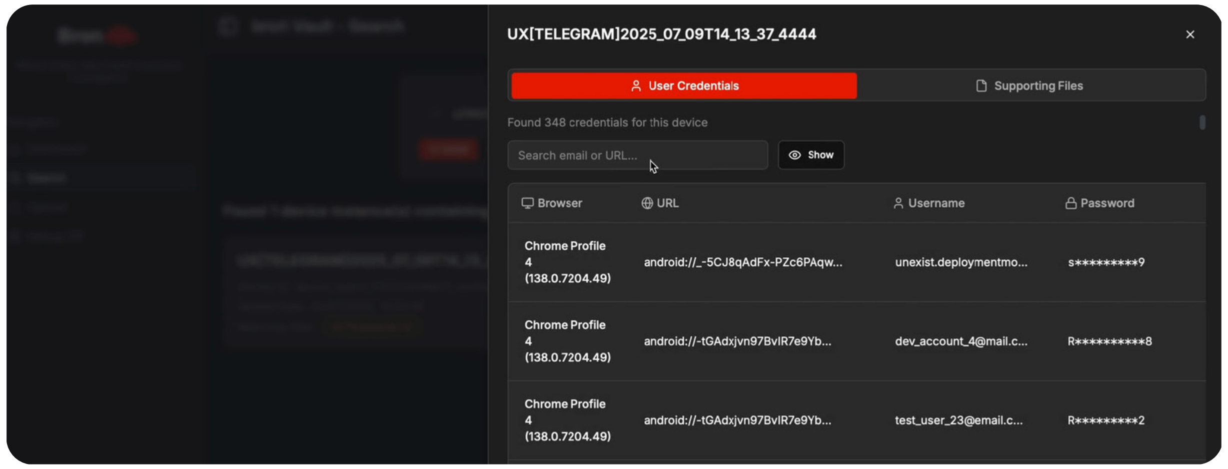
broń Vault - Search

unexist.deploymentmode1337@gmail.com

Found 1 device instance(s) containing "unexist.deploymentmode1337@gmail.com"

UX[TELEGRAM]2025_07_09T14_13_37_4444
Device ID: device_batch_1753174349571_pmhttdxmz_1753174349979_d3766dnel
Upload Date: 22/07/2025, 15:52:30
Matching files: All Passwords.txt
1 matches 272 files

Figure 17: Broń Vault - Search Feature (1)



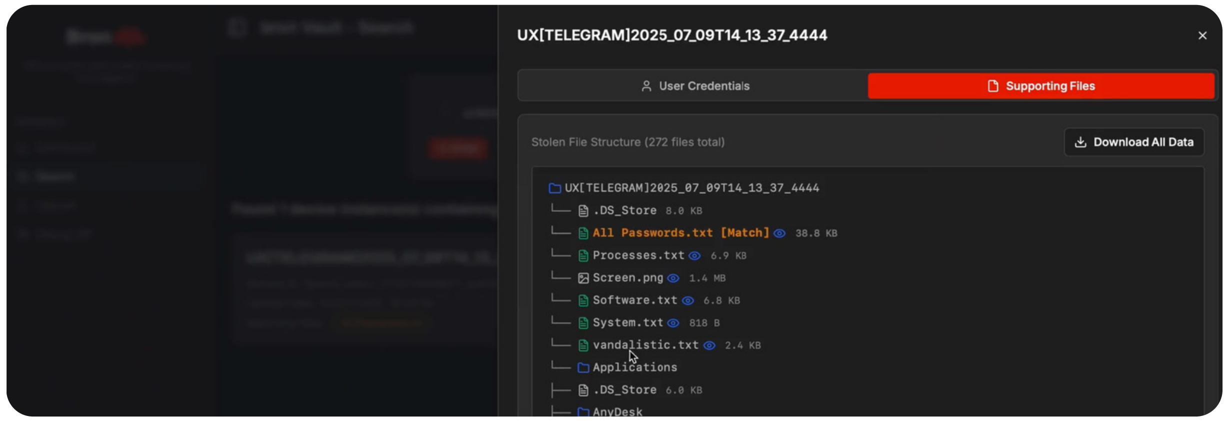
UX[TELEGRAM]2025_07_09T14_13_37_4444

Found 348 credentials for this device

Search email or URL...

Browser	URL	Username	Password
Chrome Profile 4 (138.0.7204.49)	android://_-5CJ8qAdFx-PZc6PAqw...	unexist.deploymentmo...	s*********9
Chrome Profile 4 (138.0.7204.49)	android://-tGAdxjvn97BvIR7e9Yb...	dev_account_4@mail.c...	R**********8
Chrome Profile 4 (138.0.7204.49)	android://-tGAdxjvn97BvIR7e9Yb...	test_user_23@email.c...	R*********2

Figure 18: Broń Vault - Search Feature (2)



UX[TELEGRAM]2025_07_09T14_13_37_4444

Stolen File Structure (272 files total)

```
UX[TELEGRAM]2025_07_09T14_13_37_4444
└── .DS_Store 8.0 KB
└── All Passwords.txt [Match] 38.8 KB
└── Processes.txt 6.9 KB
└── Screen.png 1.4 MB
└── Software.txt 6.8 KB
└── System.txt 818 B
└── vandalistic.txt 2.4 KB
└── Applications
├── .DS_Store 6.0 KB
├── AnyDesk
```

Figure 19: Broń Vault - Search Feature (3)

> *What used to be a painful process of connecting the dots, now becomes a seamless and intuitive workflow*

Summary and the Road Ahead

Stealer malware may not generate the same headlines as a ransomware outbreak or a zero-day exploit. This, however, is precisely what makes it so insidious. It has become a full-scale, silent epidemic, operating beneath the surface of mainstream attention, yet fueling the very attacks that do make the news.

Throughout this article, we've explored how these logs reshape both offensive and defensive operations. They offer attackers a path of least resistance around hardened defenses, and provide defenders with a raw collection of investigative leads from the compromised device. More than that, they have also raised uncomfortable questions about where the corporate security boundary truly lies, especially as personal and professional digital lives increasingly blur.

Looking forward, we also recognize that as organizations grow, their security needs often evolve towards more automated and integrated workflows. To support this very journey, our mission to democratize security extends to a dedicated technology platform and managed services designed to address these evolving needs. These solutions offer a more comprehensive approach, including large-scale data ingestion, curated threat intelligence, and proactive alerting, all designed to help teams of any size mature their security posture and stay ahead of emerging threats.

- Verizon, “2025 Data Breach Investigations Report,” Basking Ridge, NJ, USA, May 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/
- MyCERT, “MA-906.012023: MyCERT Advisory - New Dark Pink APT Group Targets Government and Military Organisations in APAC Countries,” Jan. 18, 2023. [Online]. Available: https://mycert.org.my/portal/advisory?id=MA-906.012023.
- Australian Signals Directorate, "The Silent Heist: Cybercriminals Use Information Stealer Malware to Compromise Corporate Networks," Sep. 2, 2024. [Online]. Available: https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/silent-heist-cybercriminals-use-information-stealer-malware-compromise-corporate-networks
- Y. Kho, “Understanding Stealer Logs and Their Role in Security Testing — Part 1,” Medium, Aug. 30, 2024. [Online]. Available: https://medium.com/@YoKoKho/understanding-log-stealer-and-its-role-in-security-testing-part-1-5f2223b47847
- A. Mukherjee, "How Stealer Malware Puts Your Credentials at Risk," Jul. 3, 2023. [Online]. Available: https://www.threatintelligence.com/blog/stealer-malware.
- S. Sharma and A. Kumar, "Statc Stealer: Decoding the Elusive Malware Threat," Aug.8, 2023. [Online]. Available: https://www.zscaler.com/blogs/security-research/statc-stealer-decoding-elusive-malware-threat.

INSIDE THE SOC:

EXPLORING SOC PERSONNEL AND NDR FUNCTIONS

By: Z. Ananda

> **Every second, unseen forces attempt to steal data, breach systems, and disrupt the digital lifelines we depend on. Whether we're asleep or immersed in our daily routines, a dedicated team stands watch. They're not police officers, nor soldiers—but in the cyber realm, they are the first line of defense.**

Introducing, the guardians of our digital infrastructure, working tirelessly to detect, respond, and neutralize threats before they cause harm.

Cyber threats don't wait. They slip through phishing emails, deceptive text messages, and direct assaults on server systems. The consequences? They range from financial loss and compromised corporate data to the complete shutdown of critical digital services. It's time to meet the team that keeps our digital world secure—quietly, relentlessly, and often without recognition.

Cybersecurity For Everyday Users

At the individual level, awareness is your first—and most crucial—line of defense. Cybercriminals often rely on deception: fake links, suspicious attachments, or files that appear harmless at first glance. Staying alert to these digital traps is essential.

The next layer of protection is antivirus software. Think of it as your personal security scanner, constantly checking for threats. It works by referencing a “signature file”—a database of known viruses and malware. Each file on your device is scanned and compared against this list to spot any matches.

Picture yourself as a gatekeeper with a blacklist of banned intruders. Your role? To ensure only safe files get through. That's exactly how antivirus software operates. But here's the catch: the threat landscape evolves rapidly. To stay effective, the signature file must be updated regularly—because today's malware rarely looks the same as yesterday's.

From Personal To Enterprise

Cybersecurity starts with individuals—using strong passwords, avoiding suspicious links, and installing antivirus software. But once we step into the enterprise world, the stakes skyrocket.

In corporate environments, threats are more sophisticated, targets more valuable, and the consequences of a breach far more severe. That's why companies go beyond basic tools. They invest in advanced systems that monitor everything from employee devices to the invisible highways of network traffic

Firewalls and Endpoint Detection and Response (EDR) are the first line of defense. Firewalls act like digital gatekeepers, controlling what enters and exits the network. EDR tools monitor individual devices for signs of compromise. But attackers are evolving. They now target edge devices, VPN gateways, and exploit unknown vulnerabilities—so-called zero-day threats. Traditional defenses can't always keep up.

This is where Network Detection and Response (NDR) enters the picture. Unlike EDR, which focuses on endpoints, NDR watches the entire network. It's like having surveillance cameras across every hallway, not just at the doors. By spotting unusual patterns early, NDR helps security teams respond before damage spreads.

SOC: Cybersecurity Frontline.

In enterprise environments, antivirus software and firewalls alone are no longer sufficient. A dedicated team—the SOC (Security Operations Center)—is tasked with maintaining continuous oversight and rapid response. Operating 24/7, the SOC monitors for threats such as intrusion attempts, malware propagation, and coordinated attacks.

SOC teams are typically structured into three tiers:

- Level 1 – Alarm Specialists
  The initial filter for incoming alerts, this team assesses whether a signal indicates a genuine incident or a false alarm. Unresolved or ambiguous alerts are escalated to Level 2. Their role is akin to triage—sorting routine noise from actionable threats.

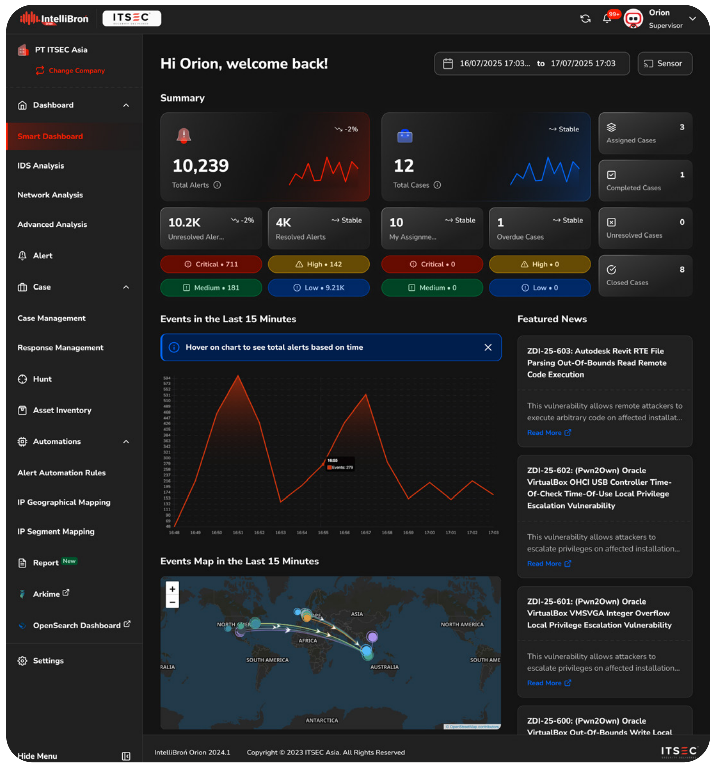
- Level 2 – Incident Responders
  Analysts at this level investigate confirmed incidents, formulate containment strategies, and restore affected systems. Complex cases requiring deeper expertise are escalated to Level 3. They function as forensic analysts, reconstructing attack vectors and impact.

- Level 3 – Threat Hunters
  This advanced tier proactively searches for vulnerabilities and emerging threats, often before any alert is triggered. They refine detection systems and handle high-severity incidents. Their role resembles strategic intelligence—anticipating and neutralizing threats before they materialize.

SOC Weapon: Network Detection Response

So far, we've met the SOC team—the digital defenders working around the clock to keep corporate systems safe. But what are the tools they rely on to spot trouble before it strikes?

As cybersecurity infrastructure grows more sophisticated—with firewalls, EDR, and NDR forming a layered defense—corporations must also ensure that threats are not just detected but decisively managed



Hi Orion, welcome back!

16/07/2025 17:03... to 17/07/2025 17:03

10,239 Total Alerts -2%

12 Total Cases Stable

3 Assigned Cases

1 Completed Cases

10.2K Unresolved Aler... -2%

4K Resolved Alerts Stable

10 My Assignme... Stable

1 Overdue Cases Stable

0 Unresolved Cases

8 Closed Cases

Critical • 711 | High • 142 | Medium • 181 | Low • 9.21K

Critical • 0 | High • 0 | Medium • 0 | Low • 0

Hover on chart to see total alerts based on time

ZDI-25-603: Autodesk Revit RTE File Parsing Out-Of-Bounds Read Remote Code Execution
This vulnerability allows remote attackers to execute arbitrary code on affected installat...

ZDI-25-602: (Pwn2Own) Oracle VirtualBox OHCI USB Controller Time-Of-Check Time-Of-Use Local Privilege Escalation Vulnerability
This vulnerability allows attackers to escalate privileges on affected installation...

ZDI-25-601: (Pwn2Own) Oracle VirtualBox VMSVGA Integer Overflow Local Privilege Escalation Vulnerability
This vulnerability allows attackers to escalate privileges on affected installation...

ZDI-25-600: (Pwn2Own) Oracle VirtualBox Out-Of-Bounds Write Local

IntelliBroń Orion 2024.1 Copyright © 2023 ITSEC Asia. All Rights Reserved

Figure 1: IntelliBroń Orion Dashboard, a network detection system, developed by ITSEC

One of the SOC's most powerful technologies is Network Detection and Response (NDR). While traditional tools like antivirus and EDR focus on individual devices, NDR shifts the lens to the entire network. It's like upgrading from a peephole to a full surveillance system—giving analysts visibility into everything moving through the digital corridors of an organization.

NDR works by placing passive sensors at strategic points in the network—often where traffic flows between endpoints, servers, and external connections. These sensors quietly collect a wealth of data, including:

- Metadata (who's talking to whom, when, and how)
- Packet captures (pcap) for deep inspection of traffic content
- Source and destination information to trace communication paths

This data is continuously analyzed to detect anomalies—unusual patterns that might indicate early-stage attacks, lateral movement by intruders, or violations of security policies. For example, if a device suddenly starts communicating with an unfamiliar server in another country, or if data begins flowing in unexpected volumes, NDR can flag it before damage is done. Unlike reactive tools that wait for something to go wrong, NDR is proactive. It's designed to catch threats in motion, often before they trigger alarms elsewhere.

Let's break them down:

1. **Search-Based Detection**
   This is the old-school, hands-on approach. SOC analysts manually look through data, hunting for signs of suspicious activity. It's incredibly accurate because every alert is verified by a human expert. But it's also time-consuming and depends on sharp eyes and experience.

> Imagine: A forensic investigator examining every fingerprint—slow but precise.

Search-based NDR is cost-effective at the platform level but the reliance on skilled analysts—or outsourced managed services—can significantly increase the total cost of ownership.

2. **Signature-Based Detection**
   This method is fast and widely used. It compares network traffic against a database of known malware "signatures." If there's a match, the system sounds the alarm. It's efficient, but has a blind spot: new threats that haven't been cataloged yet.

> Imagine: You're checking faces against a wanted list—great unless the intruder wears a new disguise.

Signature-based NDR serves is well-suited for small to medium-sized enterprises, offering cost-effective visibility with limited IT security personnel.

3. **Machine Learning-Based Detection**
   Here's where things get futuristic. This method uses AI to learn what normal behavior looks like on your network. Then it watches for anything unusual—like logins at odd hours or traffic spikes. Over time, it gets smarter, reducing false alarms and spotting threats that don't follow known patterns.

> Imagine: A behavior expert who doesn't need a list—just instincts that improve with experience.

Artificial intelligence/machine learning integration requires high-spec computing resources to process large volumes of data continuously. Naturally, this makes it the most expensive among the three detection methods.

Summary

In today's threat landscape, cybersecurity isn't just about blocking known attacks—it's about anticipating the unknown. With NDR and a skilled SOC team, organizations gain the visibility, speed, and intelligence needed to stay one step ahead.

Three approaches in detection systems—manual, signature-based, and machine learning—can be tailored to the needs and budget of the organization. In fact, combining all three is often the optimal strategy for building an effective, adaptive, and minimally disruptive detection system.

In the midst of an ever-evolving cyber threat landscape, a flexible and integrated approach is key. In next article we may explore how integrating NDR with SIEM and SOAR can elevate security operations—enabling automated, coordinated, and comprehensive responses to even the most sophisticated attacks.

The Lazarus Group's Masterstroke:

THE BANGLADESH BANK HEIST THAT SHOOK THE WORLD

By: Z. Ananda

They worked in the shadows, almost impossible to detect, until a small slip exposed everything.

There is no such thing as the perfect crime.

In 2016, a North Korean hacker group known as Lazarus came close to stealing 1 billion US dollars from the central bank of Bangladesh. Their plan was almost flawless, until one small mistake they had not considered brought the mission to a halt.

It began in January 2015, when an employee of Bangladesh Bank received what looked like a normal job application email. It was neatly written and professional, with an attachment claiming to be the CV of someone named Rasel Ahlam. Without suspecting anything, an employee clicked the link.

That simple click was the start of one of the largest cyber-attacks in banking history. The email delivered malware created by the Lazarus Group, allowing them to enter the bank's internal systems. They quietly monitored activity until they had control of vital access points, including SWIFT, the global system used for transferring funds between banks.

Over several months, Lazarus studied the bank's systems and found a weakness. On the 10th floor there was a printer that automatically printed all transactions. If this printer kept working, their illegal transfers could be discovered quickly. Lazarus hacked into the printer's control software so that it could no longer print the transaction records.

State-Sponsored Hackers: North Korea the Master Player

In the cyber world, many countries have their own hacking groups with different goals. China is known for focusing on espionage. Russia often targets high-profile systems. Iran uses cyber-attacks for political aims. However, North Korea is known for stealing money. Supported directly by their government, the Lazarus Group goes beyond spying. They focus on financial gain. Economic sanctions have pushed North Korea to find alternative sources of income through planned and systematic cyber-attacks. They are regarded as one of the most successful groups in illegally taking funds.

In this article, we're revisiting one of the most daring digital heist in history–an operation that exploited weak security system to manipulate SWIFT, a secure messaging network that is globally used to send payment instructions and other financial data.

The Federal Reserve System (The Fed) is the central bank of the United States. It manages monetary policy and helps maintain global financial stability. Many countries, including Bangladesh, keep their foreign currency reserves there because of The Fed's trusted reputation.

The Heist Begins

On Thursday, 4 February 2016, at 20:00 local time in Bangladesh, the bank was quiet. In Bangladesh, the weekend falls on Friday and Saturday, so most staff had already gone home. In New York, it was 08:36 in the morning when The Fed received instructions to transfer 951 million US dollars. The requests appeared legitimate because they were sent through the bank's official SWIFT system. The Fed found nothing unusual at first and began processing 35 transactions to accounts including the Shalika Foundation in Sri Lanka and four accounts at RCBC Bank in Manila, Philippines.

Lazarus had chosen Manila because the city has many casinos and weaker anti-money laundering regulations. They knew money sent into casinos would be very hard to trace. In May 2015, they had already opened four accounts at RCBC's Jupiter Street branch in Manila to serve as holding accounts for the stolen funds.

Meanwhile, they ensured the 10th floor printer at Bangladesh Bank remained disabled, so staff would not immediately notice the illegal transfers.

Busted by a Printer

On Friday, 5 February 2016, a bank employee realised the printer on the 10th floor was not working. As it was the weekend, no IT staff were available, and the printer problem was assumed to be a minor technical issue. The printer had broken down before, so it was not seen as urgent.

On Saturday, 6 February 2016, the IT team finally inspected the printer. The screen displayed the message “Important File Was Missing”. After several repair attempts, the printer began working again. What it printed shocked the staff. It produced records showing that almost US$1 billion had been requested for transfer from The Fed.

Panic spread. Bangladesh Bank quickly contacted The Fed, but it was too late, especially as it was also the weekend in New York. Communication delays made it harder to confirm the transactions. Some funds had already been transferred.

The Mistakes that Stopped the Heist

But amid the chaos, a glimmer of hope emerged. Although the attackers had executed a highly sophisticated operation, their plan wasn’t flawless. Two critical missteps would ultimately prevent the full heist from succeeding. The first came in the form of a simple spelling error: one of the transfer requests—worth US$20 million—was directed to the “Shalika Foundation,” but the name was misspelt as “Shalika Fundation.” That single typo triggered a reconfirmation process and finally rejection of the transaction.

The second mistake was more subtle, but just as costly. The Federal Reserve’s security systems flagged unusual activity involving multiple transactions directed to RCBC Bank’s Jupiter Street branch. The name “Jupiter” coincidentally matched that of an Iranian vessel already listed on a sanctions blacklist. This triggered an alert, prompting The Fed to block the remaining transfers before they could be processed.

Even so, Lazarus still escaped with US$81 million. Bangladesh Bank contacted the Philippine authorities to freeze the RCBC accounts, but under Philippine law a court order was required before accounts could be frozen. The situation became worse because Monday, 8 February 2016, was a public holiday in the Philippines. This extra time was used to launder the money. Within days, 50 million US dollars was moved into Manila casinos and converted into chips to make tracing harder. The rest was taken by a Chinese national named Xu Weikang.

Lessons from the Heist

The Bangladesh Bank hack is one of the most remarkable cybercrimes in modern history. How could an institution as large as The Fed, with its multi-layered security systems, be deceived by hackers from a country often seen as less advanced in technology?

This incident exposed weaknesses in international banking security, especially in the SWIFT system, which gives almost unrestricted access to anyone who manages to breach it.

What makes the case even more surprising is how carefully Lazarus planned every detail. From their technical skills to exploiting gaps in regulations in certain countries, the whole operation resembled the plot of a well-written crime film.

This event added to the long list of Lazarus Group’s victims. They continue to target opportunities for large financial gain and have recently moved into cryptocurrency theft. One case involving Lazarus targeted a crypto asset trader in Indonesia.

If they could deceive an institution such as The Fed, it is clear that many other companies could also become their next victims.

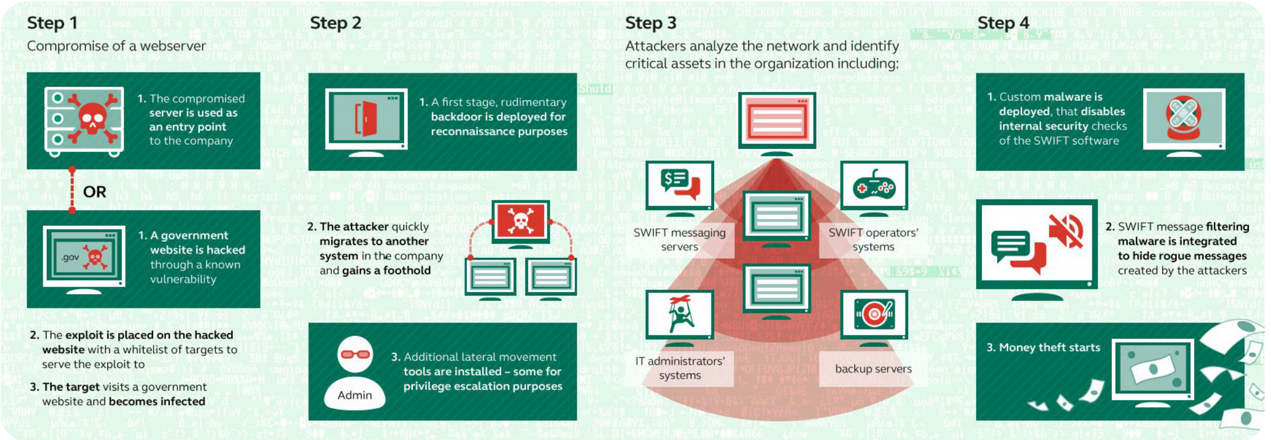
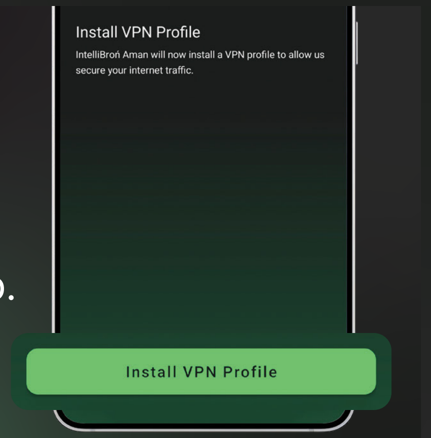
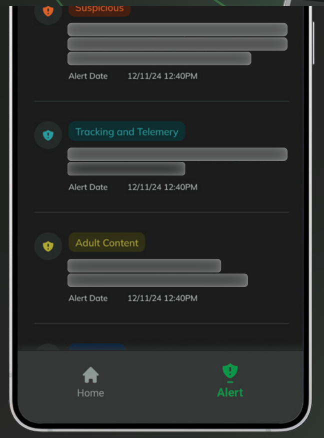
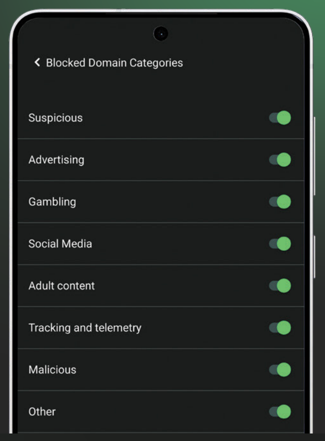

Step 1
Compromise of a webserver
1. The compromised server is used as an entry point to the company
OR
.gov
1. A government website is hacked through a known vulnerability
2. The exploit is placed on the hacked website with a whitelist of targets to serve the exploit to
3. The target visits a government website and becomes infected
Step 2
1. A first stage, rudimentary backdoor is deployed for reconnaissance purposes
2. The attacker quickly migrates to another system in the company and gains a foothold
Admin
3. Additional lateral movement tools are installed – some for privilege escalation purposes
Step 3
Attackers analyze the network and identify critical assets in the organization including:
SWIFT messaging servers
SWIFT operators’ systems
IT administrators’ systems
backup servers
Step 4
1. Custom malware is deployed, that disables internal security checks of the SWIFT software
2. SWIFT message filtering malware is integrated to hide rogue messages created by the attackers
3. Money theft starts

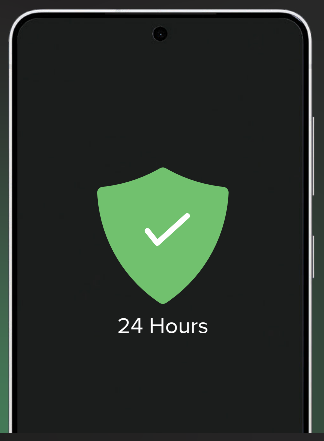
Figure 1: Lazarus Group Tactics, Techniques & Procedures of financial attack
Image by Kaspersky

Tap the button to secure your connection
Home
IntelliBroń
Your connection is secured!


Install VPN Profile
IntelliBroń Aman will now install a VPN profile to allow us secure your internet traffic.
Install VPN Profile


Suspicious
Alert Date 12/11/24 12:40PM
Tracking and Telemetry
Alert Date 12/11/24 12:40PM
Adult Content
Alert Date 12/11/24 12:40PM
Home
Alert





ITSEC CYBERSECURITY SUMMIT 2025

The Largest Critical Infrastructure Cybersecurity
Event in Southeast Asia

CONTRIBUTOR SECTION

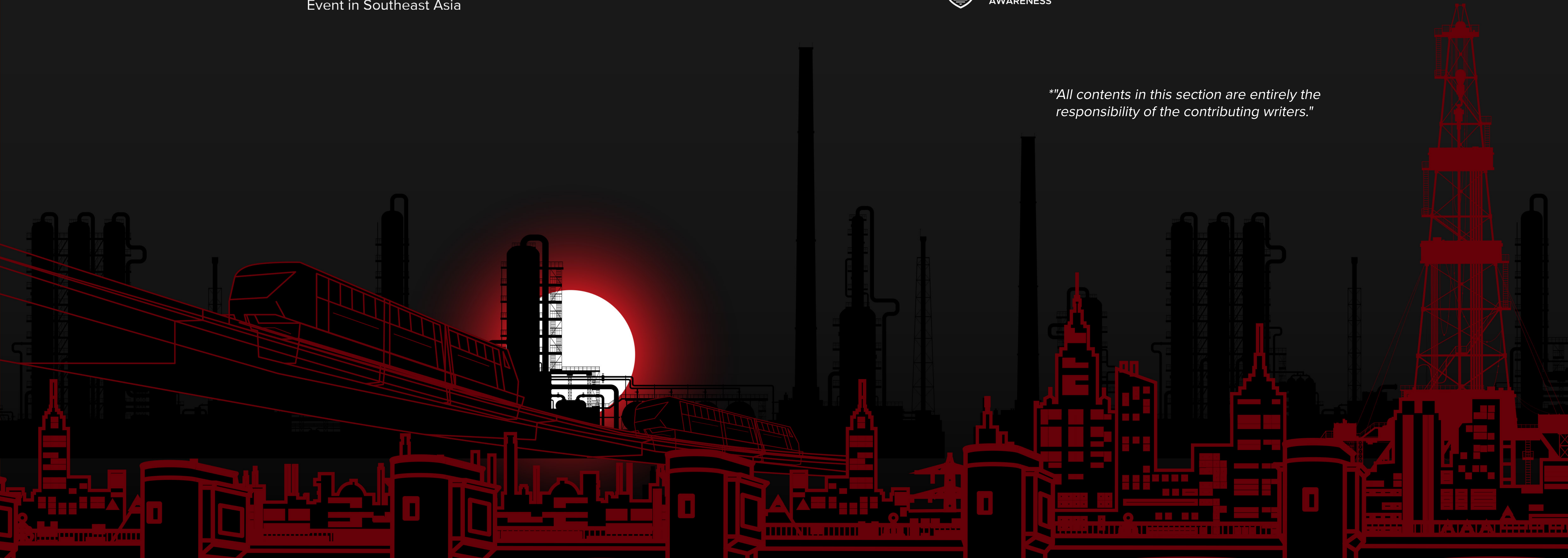
Written by:

aikido, BLACKDUCK®, mimecast®

PROMON, SOCRadar®, vicarius

LUCY AWARENESS, FORTINET, securonix

*"All contents in this section are entirely the responsibility of the contributing writers."



THE SECURITY TOOL THAT CRIED WOLF

(AND THE PROBLEM OF FALSE POSITIVES)

By Berg Severens, AI Engineer at **Aikido Security**

In the fable of the boy who cried wolf, a shepherd repeatedly raises false alarms until, when a real wolf appears, no one comes to the rescue. The sheep are lost, and everyone learns a bitter lesson about trust.

Sound familiar? It should.

Static application security testing (SAST) tools have a habit of bombarding development teams with things they don't actually need to know about. It's a global problem and, on average, up to 70% of these alerts are false positives. Alert fatigue is a real killer - distracting and draining an essential resource.

The thing is, there are threats. While industry benchmarks suggest only 42% of SAST findings are true positives, this still represents a very large number of threats knocking on the door.

The False Positive Problem

Think back to when you last looked at your security dashboard. Did it look like the inside of an F-16 cockpit? I bet it did. You probably had more alerts that you knew how to deal with. It was probably overwhelming. There's a small chance that you probably closed it after a cursory glance because there was just no indication of where to start. If you did start to wade through the alerts then well done; particularly as only a fraction of those alerts represented real threats.

This isn't conjecture. I've seen this play out many, many times. Take one recent example: a developer spends hours investigating a critical SQL injection vulnerability, only to discover it's protected by input validation that the scanner failed to recognise. Or perhaps a team delays a release to address a path traversal issue that, upon closer inspection, isn't actually exploitable.

The true cost of false positives goes beyond man-hours. There's the technical debt that stacks up. There's the fact that you're utilising a tiny portion of your best developers' skillsets. That stifles innovation and, in the worst case scenario, sees them leave the company completely. It's not unheard of for talent to head for the exit if they're restricted to doing things that aren't meaningful.

For those that do stick around, there's the danger of the "cry wolf" phenomenon. They get so used to dismissing flagged issues as false positives that they develop a reflexive "mark as resolved" habit. Then one day, buried among the noise, a legitimate vulnerability slips through. By the time anyone notices, the damage is done and the wolf is in the door.

Moving Beyond Binary Thinking

Security isn't black and white. We can't immediately categorise something as a vulnerability or not. There's a nuanced understanding needed around criteria such as exploitability, impact, and complexity.

Traditional tooling doesn't capture this nuance. It can't tell you which SQLi vulnerability is most easily exploitable, or which XSS issue touches the most sensitive data. Everything is flagged with the same urgency, leaving teams to sort through the mess with limited context.

Aside from an overhaul on tooling, the industry needs to shift its mindset of just deflecting every bullet fired from the gun. Let those that are going to miss… miss. Not all issues deserve equal attention. Some may not deserve any attention at all.

The Promise and Peril of AI Triage

The implementation of AI is a step in the right direction. Large language models offer a potential way forward. Unlike traditional rule-based systems, these models can understand code in context, recognise defensive patterns, and make more nuanced assessments about exploitability.

For example, modern AI can identify when a potential SQL injection is actually protected by an allowlist that limits inputs to specific safe values - something traditional scanners miss. In benchmark tests, advanced AI triage systems can filter out approximately 28% of false positives while still capturing 98% of genuine security debt.

But let's not be complacent. Models can make mistakes. They can misunderstand code semantics, miss novel attack patterns, or give too much weight to superficial similarities.

The solution is to augment, not automate. Arm security professionals with the tools to work more efficiently by filtering out obvious false positives and providing richer context for the issues that remain.

So how do we fix this? Here are a few concrete steps:

1. Reduce false positives with tools that understand context and can filter out alerts.
2. Integrate security into the development process. Not just a box-ticking exercise.
3. Focus on letting developers do what they love (which is building).
4. Keep your development and security processes as simple as possible.

Most importantly, start measuring impact smartly - the number of vulnerabilities detected should never be a KPI.

AI Avalanche: TAMING SOFTWARE RISK WITH TRUE SCALE APPLICATION SECURITY

By Black Duck

Software is an essential driver of growth and innovation for every company. Its criticality is never in question. But the old software world is gone, giving way to a new set of truths defined by AI and global software regulations. On the one hand, as AI adoption surges, an avalanche of AI-generated code presents new threat landscapes. On the other hand, accountability and compliance is increasingly a core requirement of doing business.

Consider that software today is:

- **Bigger** The average application has three times more code than it did four years ago.
- **Growing** By 2030, there will be three times more applications than there are today.
- **Under attack** Global cyberattacks continue to proliferate, with a 30% increase last year, reaching an average of over 1,600 attacks per organization per week.
- **More regulated** Intensifying pressure from industries and governments to comply with regulatory requirements make accountability and transparency table stakes for doing business.

With AI-generated code projected to grow by 400% by 2030, the risks are only going to accelerate and compound, threatening IP leakage, innovation stagnation, financial exposure, development sinkholes, and regulatory showstoppers.

It's simply no longer tenable to have to choose between speed and accuracy, innovation velocity and compliance rigor, budget realities and full-integrity assurance, and AppSec scale and time-to-market.

> ***So how will your organization meet the exponential demands on software development in this regulated, AI-powered world?***

True Scale Application Security

When it comes to application security solutions, it's no longer about "good enough" find-and-fix tools, offloading security with a shift-left approach, or CI/CD where security is an afterthought. These solutions create gaps and friction, and they weren't built to handle the scale, speed, and regulatory pressure of the new software world.

Black Duck is able to meet the demands of modern software with True Scale Application Security, ensuring uncompromised trust in software while achieving unparalleled protection and efficiency—in the cloud, on premises, and in hybrid environments.

We Deliver

- **Speed at scale.** Rapidly develop, deploy, and manage applications regardless of size or the volume of data and users.
- **Accuracy at scale.** Development speed compromises your business if it causes you to miss issues or stop to address inaccurate results. Maintaining high levels of precision and reliability across applications of all shapes and sizes is critical. Black Duck offers industry-leading analysis engines with multifactor scanning that provide unmatched accuracy and fidelity.
- **Volume at scale.** Speed and accuracy can't break down when large volumes of data, users, and applications need to be secured. Black Duck can handle the hyper growth and proliferation of enterprise applications.
- **Compliance at scale.** Consistent and rigorous compliance practices are necessary to adhere to all relevant legal, regulatory, and industry standards as your organization's applications grow and multiply. Black Duck provides comprehensive open source management, dynamic security testing, advanced analytics, and seamless integration into the SDLC to ensure that our customers meet all regulatory requirements.

Obliterating The Status Quo

By removing the tradeoffs between speed, accuracy, and compliance We're turning security bottlenecks into innovation accelerators. We're turning code testing into risk prioritization. Instead of scanning 10 times the lines of code that's 90% open source, our tools scan hundreds of times the lines of code that's 90% AI-generated.

We've replaced incomplete views of software components with comprehensive, compliance-ready views. And instead of introducing risk for the sake of increased developer productivity, we're delivering development velocity with trust.

Taming risk in a regulated, AI-powered world

To tame risk in this new era of proliferating software, we've identified seven requirements that every organization in the world should adopt.

- Make application security an executive mandate
- Prepare for AI scalability
- Avoid regulatory pitfalls that delay innovation and delivery
- Safeguard your full SDLC
- Boost decisioning superiority and eliminate tradeoffs
- Drive precision and ease of use
- Start anywhere your code happens

The next frontier of AppSec is here to meet the exponential demands of modern software in a regulated, AI-powered world.

True Scale Application Security reduces the exposure of mission-critical software to the security, regulatory, and licensing risks that cause failure or impede time-to-market.

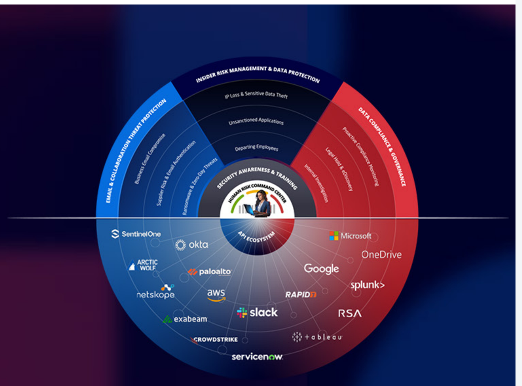
Security leaders can make smarter decisions, freeing organizations from outdated tradeoffs between speed, accuracy, and compliance—at the scale their businesses need, delivering development velocity with trust.

BLACKDUCK ITSEC: Cybersecurity Summit 2025 Sponsor

MIMECAST HUMAN RISK COMMAND CENTER TO PROVIDE UNPRECEDENTED VISIBILITY AND RISK MITIGATION FOR ORGANIZATIONS

By **Mimecast**

Mimecast, a global cybersecurity leader transforming the way businesses manage and secure human risk, unveiled the first-of-its-kind Human Risk Command Center. This innovative addition to Mimecast's **Human Risk Management (HRM)** platform equips organizations with unparalleled visibility into human risk, enabling them to identify and mitigate threats more effectively and efficiently.


INSIDER RISK MANAGEMENT & DATA PROTECTION
IP Loss & Sensitive Data Theft
Unsanctioned Applications
Departing Employees
EMAIL & COLLABORATION THREAT PROTECTION
Business Email Compromise
Supplier Risk & Email Authentication
Ransomware & Zero-Day Threats
DATA COMPLIANCE & GOVERNANCE
Proactive Compliance Monitoring
Legal Hold & eDiscovery
Internal Investigation
SECURITY AWARENESS & TRAINING
HUMAN RISK COMMAND CENTER
API ECOSYSTEM
SentinelOne
okta
ARCTIC WOLF
paloalto
netskope
aws
exabeam
slack
CROWDSTRIKE
servicenow
Microsoft
OneDrive
Google
splunk>
RAPID7
RSA
tableau

The Human Risk Command Center is engineered to include:

- **Advanced Risk Scoring:** Assigns risk scores to users, empowering security teams to prioritize efforts on the most vulnerable points within their human network.
- **Integrated Security Intelligence:** Leverages both Mimecast data and a wealth of third-party security solutions, including key partnerships to provide deeper visibility and actionability into human risk factors.
- **Proactive Interventions:** Powered by Mimecast Engage® technology, the revolutionary adaptive security awareness solution, customers can use tailored security interventions, including real-time Slack notifications and personalized behavioral nudges to correct risky behaviors and reinforce secure practices.
- **Precision Detection:** Actionable insights obtained from the command center will enable CISOs and security analysts to make informed decisions and quickly deploy the right tactics to protect the organization.
- **Streamlined Data Management and Compliance:** The command center will also continue to advance and improve after the initial launch. One future advancement will be helping organizations identify and address non-compliance and data loss in collaboration tools through Mimecast Aware. By securing collaboration data at scale, companies can ensure compliance while accelerating incident response times.

Marc van Zadelhoff, CEO of Mimecast stated:

> *"Human risk is a pervasive challenge that all organizations must tackle head-on. Our Human Risk Command Center is a major step forward, providing the tools necessary to measure human risk, empower employees as defenders, and protect customers from sophisticated targeted attacks. This innovation helps simplify the complexity of managing human risk."*

The Power of Together – Greater Human Risk Visibility and Protection Through Integration

Mimecast's expanding technology alliance program now includes more than 6,000+ connected customers, 300+ integrated applications and 1.3B+ API calls every month. The Mimecast Technology Alliance Program features integrations with some of the industries most renowned companies. These collaborations enhance automated protection, detection and integrated response.

Highlighting their commitment to accessibility, Mimecast solutions are now available on the AWS Marketplace. This simplifies the purchasing and deployment process for Mimecast customers, allowing them to more easily leverage the Mimecast platform. In December 2024, Mimecast was named a winner of the Rising Star Technology Partner of the Year for EMEA award by AWS.

Analyst Recognition and Confirmation

In recent months Mimecast's vision and product development has been recognized in key analyst reports. Including a 'Strong Performer' distinction in the Forrester Wave™: Human Risk Management Solutions, Q3 2024, and a 'Leader' placement in both the 2024 Gartner® Magic Quadrant™ for Email Security Platforms and the 2025 Gartner® Magic Quadrant™ for Digital Communications Governance and Archiving Solutions. For more information visit here.

About Mimecast

Mimecast is a leading cybersecurity company transforming the way businesses manage and secure human risk. Its AI-powered, API-enabled connected human risk platform is purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight.

By enabling decisive action and empowering businesses to protect their collaborative environments, our technology safeguards critical data and actively engages employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape.

From insider risk to external threats, customers get more with Mimecast. More visibility. More agility. More control. More security.

mimecast

ITSEC: Cybersecurity Summit 2025 Sponsor

MOBILE APPLICATION SECURITY:

Understanding Threats, Standards and Effective Solutions

By Eric Iswara, Engineer of Promon AS

Mobile application security encompasses strategies and technologies to protect mobile apps from cyber threats, data breaches, and unauthorized access. As mobile devices become primary tools for digital tasks, securing apps is critical due to their access to sensitive data and vulnerabilities across platforms like Android and iOS.

Mobile apps face diverse threats, often exploiting vulnerabilities in code, communication, or user behaviour;

- Data breaches: Insecure data storage or weak encryption can expose sensitive information.
- Phishing and malware: Fake apps (e.g., FjordPhantom running banking Apps in virtual environment) trick users into sharing credentials. Snowblind bypassing all security checks on the Android operating system.
- Code tampering and reverse engineering: Reverse engineering involves decompiling and analyzing the compiled app files (APKs for Android and IPAs for iOS) to understand an app's structure, functionality, and vulnerabilities.
- Session hijacking: Exploiting active sessions to breach company's application.

Security Standards and Frameworks to combat these risks, organizations should adopt standards such as:

- OWASP Mobile Application Security Verification Standard (MASVS)
- Digital Operational Resilience Act (DORA)
- Cyber Security Agency of Singapore – Safe App Standard
- NIST Cybersecurity Framework 2.0

Effective Mitigation Strategies include:

- Secure coding practices: Encrypting data, implementing robust authentication, and validating inputs.
- Regular security assessments: Network analysis, third-party dependency checks, and penetration testing.
- Runtime protection: Runtime Application Self-Protection (RASP) solutions to detect and block malware in real time.
- Continuous monitoring: Periodic updates, patch management, and post-remediation testing.

By integrating these standards and practices, developers and organizations can mitigate risks while maintaining user trust in an increasingly mobile-centric world.

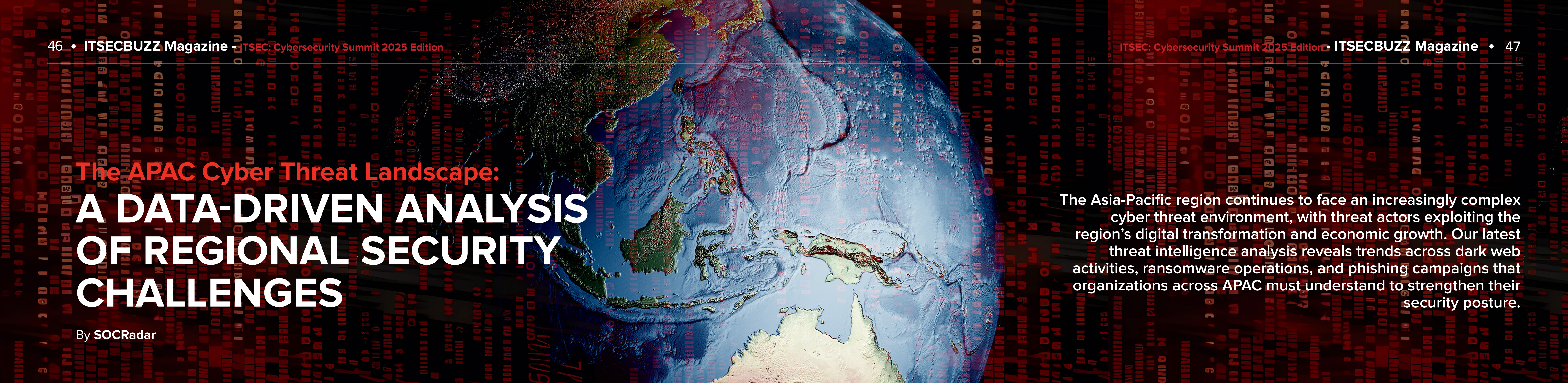
About Promon AS:

Promon is a Norwegian firm specialising in App Hardening, with our solutions focusing largely on Runtime Application Self-Protection (RASP). The company works with a variety of global Tier 1 clients, counting customers in industries such as finance, gaming, health and the public sector. Promon's technology originates from the internationally recognized research environments at SINTEF and the University of Oslo. Promon's patented deep protection technology Promon SHIELDTM, has protected apps and applications used by more than 2 Billion users. Promon AS is a Norwegian limited company registered in 2006, with offices in Hong Kong, Germany, the UK, the US and India.

PROMON

ITSEC: Cybersecurity Summit 2025 Sponsor

www.promon.io

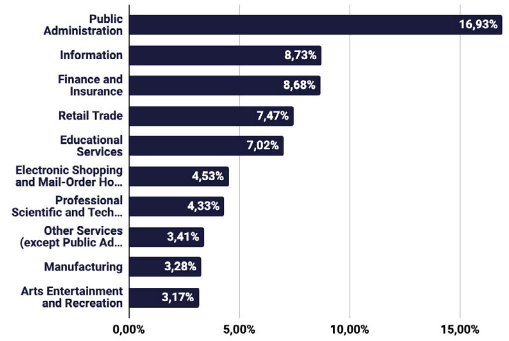


The APAC Cyber Threat Landscape: A DATA-DRIVEN ANALYSIS OF REGIONAL SECURITY CHALLENGES

By **SOCRadar**

The Asia-Pacific region continues to face an increasingly complex cyber threat environment, with threat actors exploiting the region's digital transformation and economic growth. Our latest threat intelligence analysis reveals trends across dark web activities, ransomware operations, and phishing campaigns that organizations across APAC must understand to strengthen their security posture.

Dark Web Threats: GOVERNMENT AND FINANCIAL SECTORS UNDER SIEGE

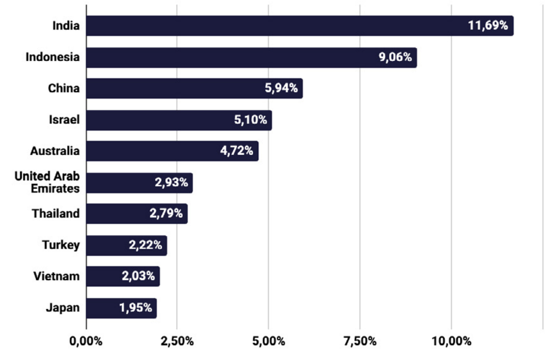


Picture: **Distribution of Dark Web Threats by Industry**

Our analysis of dark web threat distribution reveals that **Public Administration leads as the most targeted sector**, accounting for 16.93% of all threats targeting APAC. This concentration on government entities reflects the high value of political intelligence and citizen data.

The financial sector faces substantial pressure, with **Finance and Insurance organizations representing 8.68% of threats.** The convergence of these statistics with the 4.53% targeting of **Electronic Shopping and Mail-Order Houses** demonstrates threat actors' clear focus on sectors handling sensitive data.

Geographic Distribution: INDIA AND INDONESIA LEAD REGIONAL TARGETING



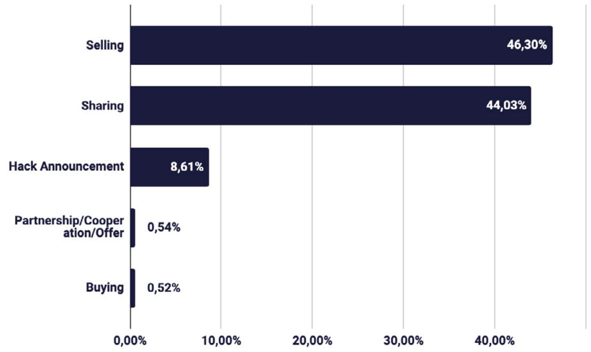
Picture: **Distribution of Dark Web Threats by Country**

From a geographic perspective, **India dominates the threat landscape with 11.69% of all dark web threats**, followed by **Indonesia at 9.06%.** These figures likely reflect both countries' large digital populations and rapidly expanding digital economies, making them attractive targets for threat actors.

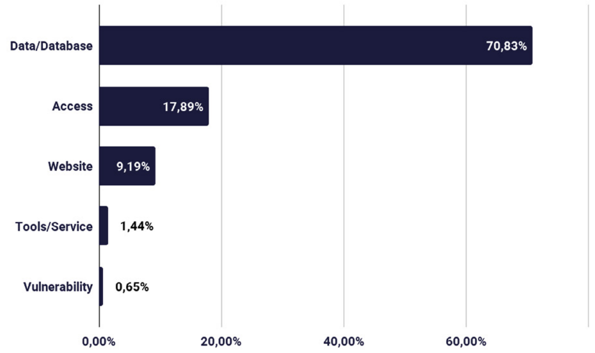
China's 5.94% share is particularly noteworthy given its sophisticated cyber defense capabilities, while **Israel's 5.10% representation** suggests the country's strategic importance extends beyond traditional geopolitical considerations into cyberspace.

Australia rounds out the top five at 4.72%, reflecting its position as a developed economy with substantial digital infrastructure.

Threat Actor Behavior: DATA THEFT DOMINATES CRIMINAL ACTIVITIES



Picture: **Distribution of Dark Web Threats by Threat Categories**

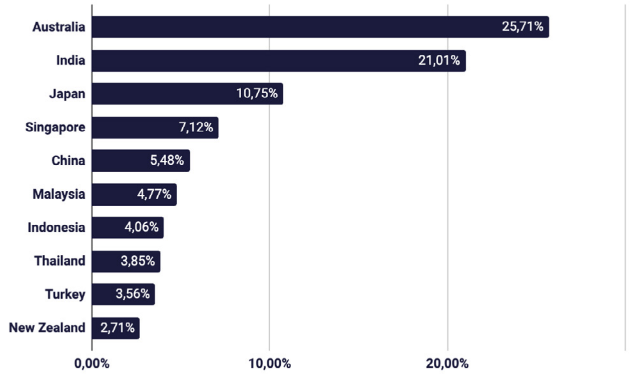


Picture: **Distribution of Dark Web Threats by Threat Types**

The analysis reveals that **cybercriminals primarily engage in selling activities (46.30%) and sharing stolen data (44.03%).** This near-equal split between selling and sharing suggests a mature underground economy where threat actors both monetize stolen data and build reputation through information sharing.

Data and database theft accounts for an overwhelming 70.83% of threat types, with access credentials representing 17.89%. This pattern indicates that threat actors prioritize obtaining bulk data over targeted website compromises (9.19%) or specialized tools and services (1.44%).

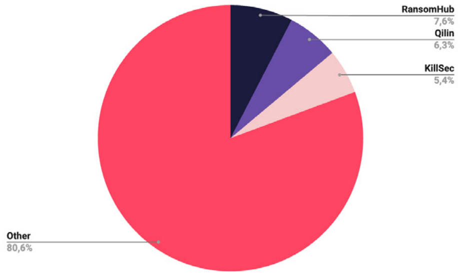
Ransomware:
AUSTRALIA AND INDIA BEAR THE BRUNT



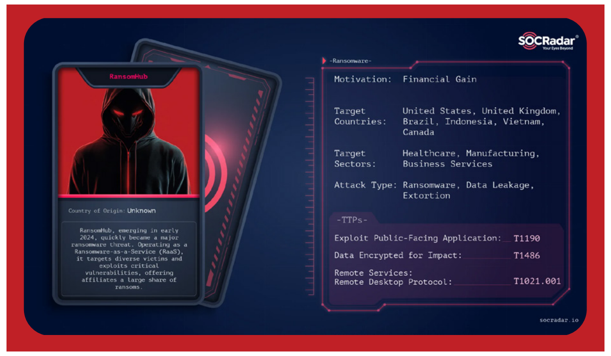
Picture: **Distribution of Ransomware Attacks by Target Country**

Ransomware operations show a concentrated pattern, with **Australia suffering 25.71% of attacks and India experiencing 21.01%.** Australia's high percentage suggests that its developed economy and digital infrastructure make it particularly attractive to ransomware operators seeking maximum financial impact.

Japan's 10.75% share reflects ongoing targeting of the country's technology sector and critical infrastructure. The emergence of **RansomHub (7.60%), Qilin (6.30%), and KillSec (5.40%)** as leading groups demonstrates the fragmented but persistent nature of ransomware operations in the region.



Picture: **Top Ransomware Groups Targeting APAC**



RansomHub

Country of Origin: Unknown

RansomHub, emerging in early 2024, quickly became a major ransomware threat. Operating as a Ransomware-as-a-Service (RaaS), it targets diverse victims and exploits critical vulnerabilities, offering affiliates a large share of ransoms.

-Ransomware-

Motivation: Financial Gain

Target Countries: United States, United Kingdom, Brazil, Indonesia, Vietnam, Canada

Target Sectors: Healthcare, Manufacturing, Business Services

Attack Type: Ransomware, Data Leakage, Extortion

-TTPs-

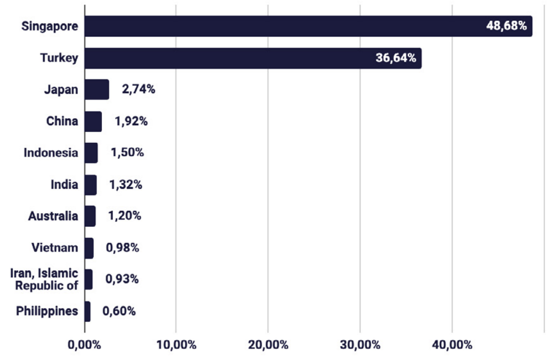
Exploit Public-Facing Application: T1190

Data Encrypted for Impact: T1486

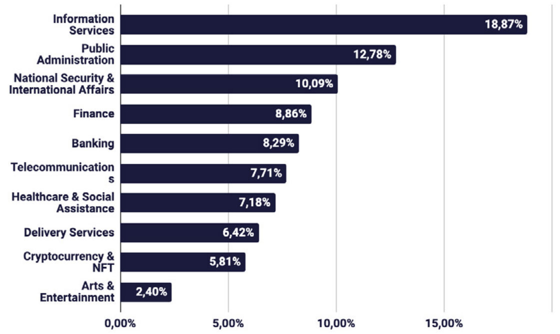
Remote Services: Remote Desktop Protocol: T1021.001

socradar.io

Phishing Campaigns:
SINGAPORE EMERGES AS PRIMARY TARGET



Picture: **Distribution of Phishing Attacks by Country**

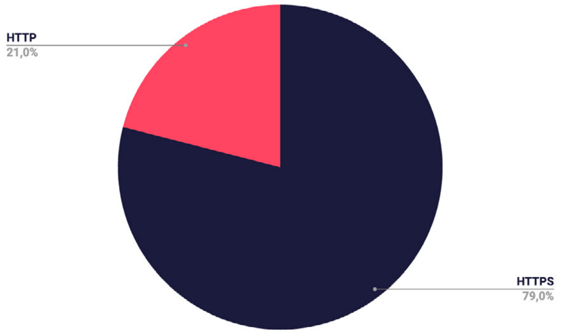


Picture: **Distribution of Phishing Attacks by Industry**

Perhaps most striking is **Singapore's dominance in phishing attacks, accounting for 48.68% of all observed campaigns.** This concentration likely reflects Singapore's position as a regional financial hub and the presence of numerous multinational corporations with valuable corporate data.

Turkey's significant 36.64% representation in phishing attacks suggests threat actors view the country as a gateway between European and Asian markets. The **Information Services sector leads phishing targets at 18.87%,** followed by **Public Administration at 12.78%,** indicating cybercriminals' preference for high-value data repositories.

The prevalence of **HTTPS protocols in 78.98% of phishing sites** demonstrates threat actors' sophistication in creating legitimate-appearing malicious infrastructure, making detection more challenging for both security tools and end users.



Picture: **Distribution of Phishing Attacks by SSL/TLS Protocol**

Strategic Implications and Recommendations

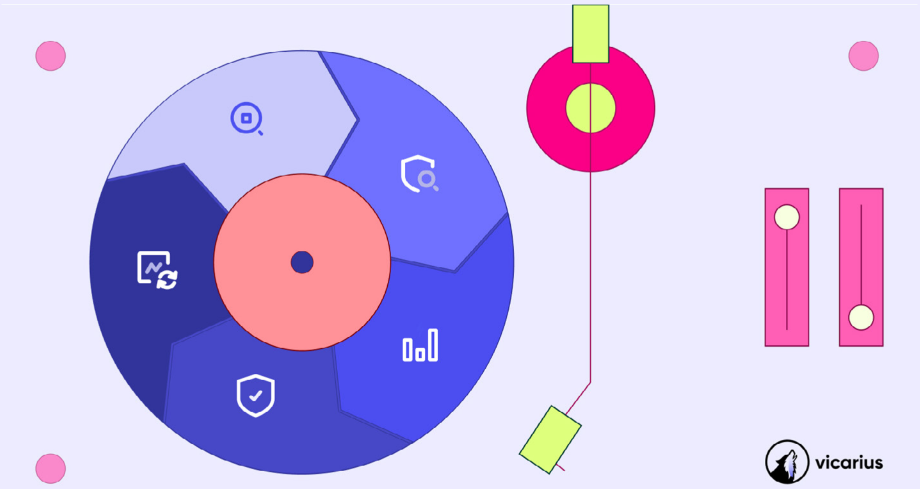
Organizations across APAC must adopt a threat-informed security strategy that accounts for these regional patterns while maintaining vigilance against emerging threat vectors. The sophisticated nature of observed campaigns, from encrypted phishing infrastructure to organized ransomware operations, requires equally sophisticated defensive measures.

As the region continues its digital transformation journey, understanding and adapting to these threat patterns will be crucial for maintaining economic growth while protecting critical digital assets and citizen data.

Vulnerability Remediation:

COMPLETE PROCESS, CHALLENGES, AND AUTOMATED BEST PRACTICES

By: Sagy Kratu, Sr. Product Marketing Manager **at Vicarius**



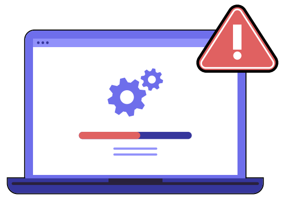
Finding vulnerabilities is easy. Fixing them is not.

Every organization has scanning tools lighting up dashboards with CVEs, misconfigurations, and outdated libraries. But unless you close the loop with remediation, those alerts remain just that. Attackers don't wait for patch cycles or committee approvals. They exploit.

That's why vulnerability remediation is where cybersecurity moves from visibility to action. It's the stage where risk is reduced, threats are blocked, and security becomes measurable.

In this guide, we'll walk through the entire vulnerability remediation process from discovery to validation and show how modern teams overcome the challenges of scale, complexity, and resource constraints. You'll also see how automation and tools like Vicarius vRx make proactive, policy-driven remediation possible.

What Is Vulnerability Remediation?



Vulnerability remediation is the process of identifying, prioritizing, and fixing security weaknesses in systems, software, or configurations to prevent exploitation.

It's not just about patching. It's about making targeted, risk-aware decisions to reduce exposure before attackers can take advantage of it.

Putting Remediation in Context: One Step in a Bigger Strategy

Remediation doesn't live in a vacuum. It's part of the larger vulnerability management lifecycle, which includes:

1. **Discovery:** Uncovering vulnerabilities across assets, endpoints, servers, cloud, containers.
2. **Assessment:** Understanding severity, context, and potential business impact.
3. **Prioritization:** Deciding what to remediate now, what to monitor, and what can be mitigated.
4. **Remediation:** Taking corrective action, whether patching, reconfiguring, or shielding.
5. **Validation:** Verifying that remediation worked and risk is actually reduced.
6. **Reporting:** Documenting actions for compliance, audits, and internal performance tracking.

Each stage feeds the next. But without effective remediation, the entire cycle breaks and attackers exploit the gap between visibility and action.

The Vulnerability Remediation Process: Step-by-Step

STEP 1 Identification

It starts with visibility. Security scanners detect vulnerabilities across the environment, from outdated operating systems to misconfigured cloud permissions. Most of these are mapped to known CVEs. Others might come from vendor advisories or internal discovery.

You'll often find:

- Missing OS or third-party patches
- Unsafe open ports or weak configurations
- Unsupported software still in use
- Supply chain exposures via embedded components

A good identification process captures what's vulnerable, where, and how it matters. But it doesn't yet tell you what to do.

STEP 2 Prioritization

This is where most teams get stuck. You scan 5,000 assets and find 30,000 vulnerabilities. Where do you begin?

Modern remediation requires risk-based prioritization not just fixing the "highest CVSS score," but understanding:

- Is there a known exploit in the wild?
- Is the vulnerable system business-critical?
- Is it internet-facing?
- Are compensating controls already in place?

Threat intelligence plays a big role here. A low-CVSS vulnerability with an active ransomware exploit is more urgent than a 9.8 CVE buried on an isolated test machine.

Risk-based scoring, exploitability flags, asset context, and patch availability all feed into prioritization tools and this is where platforms like Vicarius excel. The goal is simple: fix what matters most, first.

STEP 3 Fix or Mitigate

With your priorities set, it's time to act.

Remediation may involve:

- Applying vendor patches across OS and application layers
- Changing configurations (e.g., disabling weak ciphers, restricting access)
- Deploying virtual patches for zero-days or unpatchable systems
- Replacing or upgrading unsupported software
- Segmentation or isolation if remediation is not immediately possible

In some cases, you can't fully remediate right away. That's where mitigation comes in adding controls (firewall rules, monitoring, access restrictions) that reduce risk until a full fix is feasible.

And yes, some vulnerabilities should be accepted. But that should be a decision not the default due to backlog or fatigue.

STEP 4 Validation and Documentation

Fixing a vulnerability is not the end of the process. Verifying the fix is just as important.

Validation includes:

- Re-scanning the asset to confirm the vulnerability is resolved
- Logging the fix in ticketing systems or vulnerability platforms
- Documenting timelines, actions, and responsible teams
- Measuring time-to-remediate (MTTR) and other KPIs

This isn't just for compliance. It's about building a system you can trust and prove to others.

Why Remediation Is So Hard: 6 Common Challenges

Every security team wants to remediate quickly and effectively. But the reality is harder.
Here are the obstacles most teams face:

1. Patch Overload
Thousands of vulnerabilities, limited time. Most teams don't have enough bandwidth to handle the volume and "critical" is a moving target.

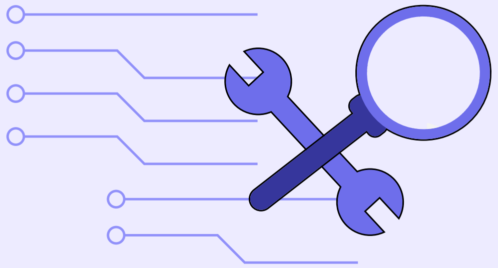
2. Change Management Bottlenecks
Fixes require approvals. In some orgs, patching a production server is harder than deploying new features. Change windows are rare, and rollback planning adds friction.

3. Fragmented Tooling
Scanning, patching, scripting, and ticketing often happen in different tools. That creates gaps or worse, manual workarounds that don't scale.

4. Legacy and Unpatchable Systems
Old hardware or software may not support updates. Teams are left to isolate or virtual-patch instead.

5. Lack of Ownership
Is it IT's job or Security's? Who owns remediation for third-party apps? Role clarity is often missing.

6. Compliance Pressure
Security teams must meet external patching deadlines (HIPAA, PCI-DSS, ISO), but business units resist downtime. It's a constant balancing act.



Best Practices: Making Remediation Work at Scale

Successful remediation programs aren't perfect; they're consistent, transparent, and prioritized.

Here's what they do well:

Embrace Risk-Based Prioritization - Shift from patch-all to patch-what-matters. Prioritize based on exploitability, business value, and exposure.

Define Roles and Ownership - Clear SLAs. Clear owners. Make it obvious who's responsible for remediation by system, application, or business unit.

Align with IT and Change Windows - Security can't act alone. Align remediation plans with scheduled maintenance and IT workflows to avoid friction.

Test, Rollout, and Rollback - Use phased deployments. Test in staging. Always have a rollback plan in case something breaks.

Automate Where You Can - Free your team from low-value, repetitive tasks. More on this in a moment.

Track and Report - Monitor MTTR. Track % of high-risk vulns resolved within SLA. Identify bottlenecks and fix them.

Automation and Preemptive Remediation with Vicarius

Manual remediation can't keep pace with today's threat velocity. That's why automation is no longer a nice-to-have; it's essential.

Vicarius vRx makes automated, intelligent remediation a reality by:

- Patching across operating systems and 10,000+ third-party applications
- Running script-based fixes for misconfigurations or policy enforcement
- Applying patchless protection when no patch exists, using memory-level shielding
- Automating policy-based remediation based on exploitability, risk score, or asset type
- Tracking every action for audit and compliance reporting

You set the guardrails vRx takes action when conditions are met. This eliminates delay, reduces error, and turns remediation into a proactive security control.

Gartner calls this the future of security operations. We call it the new normal.

Remediation Metrics That Matter

Tracking the right metrics drives visibility and accountability.

- Mean Time to Remediate (MTTR)
- % of critical vulnerabilities resolved within SLA
- Top 10 recurring CVEs by asset group
- Remediation volume by month or team
- Time to patch vs time to exploit (TTP-TTE gap)

These numbers tell you where you're improving, where you're stuck, and where automation could help most.

Final Thoughts: From Visibility to Impact

> **It's easy to get lost in dashboards and detections. But security isn't about knowing what's vulnerable—it's about doing something about it.**

Vulnerability remediation is where that happens. It's how you reduce real-world risk. It's how you meet compliance. It's how you win time back for your team.

When done right and especially when automated with platforms like Vicarius vRx remediation becomes a strength, not a bottleneck.

So don't just scan. Don't just triage. Remediate with intent, with speed, and with confidence.

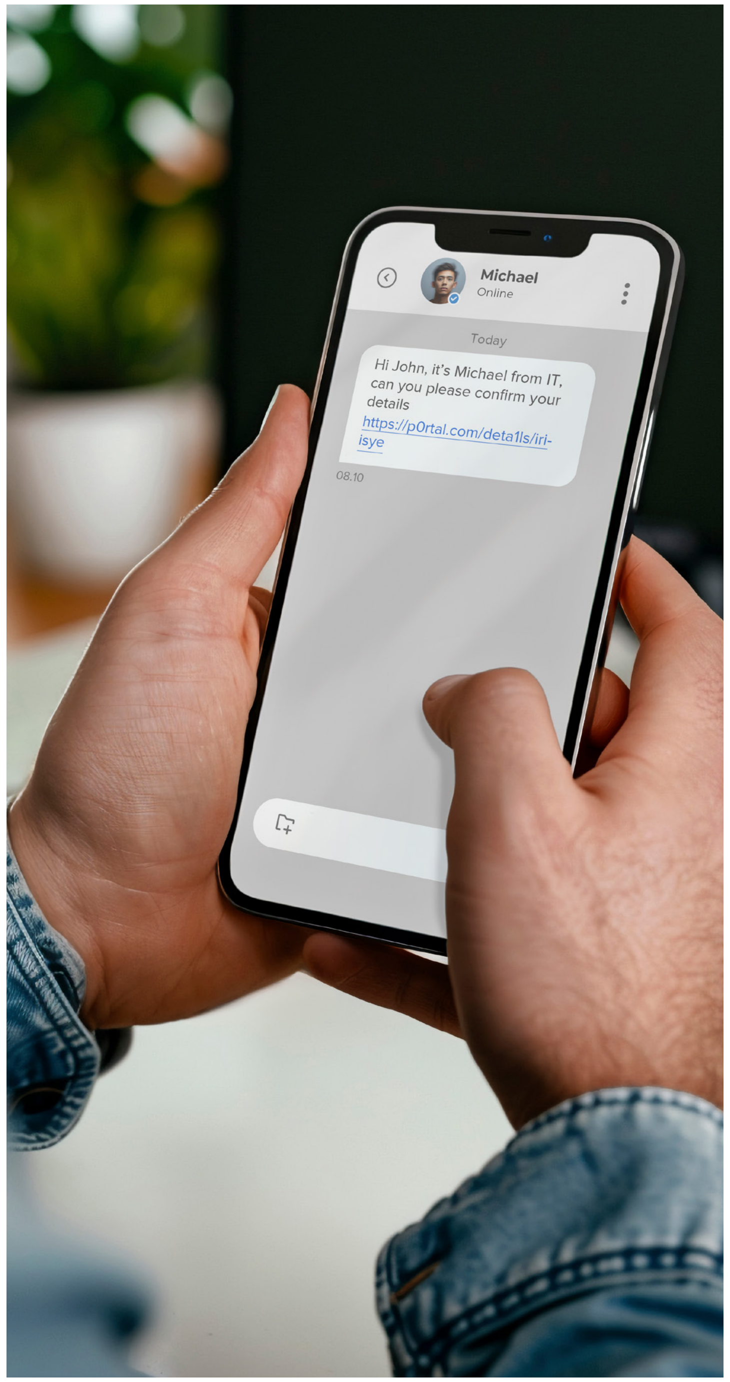
vicarius

ITSEC: Cybersecurity Summit 2025 Sponsor

WHY PHISHING REALISM MATTERS:

Testing Defenses with Attacks That Look-and Feel-Real

By Clifford Ang
Regional Sales Director for Asia at Lucy Security



Michael
Online
Today
Hi John, it's Michael from IT, can you please confirm your details
https://p0rtal.com/deta1ls/iri-isye
08:10

In 2025, phishing has evolved far beyond suspicious emails and dubious links. In Southeast Asia—where mobile-first usage, messaging apps, and digital acceleration are booming—cybercriminals are matching their techniques to local habits, languages, and platforms. That makes simulated phishing campaigns harder to get right—and all the more important to get real.

It's time for organizations to stop testing users with outdated or generic email lures and start simulating the actual threats targeting their networks. Because real attackers don't follow templates—and neither should you.

Phishing is Evolving in SE Asia

In markets like Singapore, Indonesia, Thailand, and Malaysia, phishing campaigns are becoming hyper-realistic and platform-diverse. Our customers across Southeast Asia report a high level of activity for social engineering fraud, with messaging-based scams in particular growing rapidly due to high smartphone and mobile payment usage.

Attacks today are not only personalized—they're persistent. Cybercriminals are repurposing real company branding, mimicking internal HR or finance messages, and increasingly using mobile channels like SMS and WhatsApp to bypass traditional email filters.

Recent high-profile trends include the spike in SMS-based scams in Singapore impersonating government agencies and banks and WhatsApp based job scams, particularly in Thailand. These aren't hypothetical risks—they're daily realities for regional businesses and are resulting in losses into the millions.

Beyond Email — Training for Smishing and WhatsApp Threats

The rise of smishing (SMS phishing) and phishing via messaging platforms like WhatsApp has exposed a gap in most organizations' awareness programs: they're still training users to spot threats in inboxes, while attackers are already in their message threads.

Modern awareness programs need to simulate threats across **all relevant channels**—not just email. That means testing employee responses to convincing SMS messages with embedded links, or WhatsApp messages that mimic real conversations from colleagues or vendors.For example, a simulated smishing message might appear to come from your bank's fraud team, urging immediate action. A WhatsApp phishing simulation could replicate a team lead's request to approve a payment "urgently." If your people aren't seeing these simulations during training, how will they respond in real life?

Clone and Repurpose — Real Attacks as Training Material

The best way to simulate a phishing attack? Use one that already worked—or nearly did.

Modern awareness platforms now allow **attack cloning:** the ability to take real phishing emails, sanitize them, and re-use them in simulations tailored to your organization. But Lucy Security goes a step further—we enable **cloning of landing pages too.** That means your simulation doesn't just copy the phishing email—it mimics the malicious website it links to.

Why does this matter? Because attackers are mimicking everything: Microsoft 365 login pages, bank portals, e-signature requests, payment systems. If users can't tell the difference between a real page and a cloned one, your simulations should reflect that challenge.

By using cloned attack components, you can test real scenarios your employees are likely to face—without the guesswork.

What "Realism" Achieves

Realistic phishing training isn't about fear—it's about preparing people for how attackers really operate.

LUCY AWARENESS

Smarter simulations. Faster threat response. Safer culture

Overly simplistic training with fake Amazon receipts or cartoonish Nigerian prince emails may tick a compliance box, but they won't change behavior.

When phishing simulations mirror real-life lures—same style, same tone, same urgency—users engage more critically. That drives higher awareness, better reporting rates, and measurable risk reduction.For regional firms, this realism also means cultural and linguistic accuracy. Attack simulations must reflect local norms—like Malay, Thai, or Tagalog messaging patterns, mobile payment requests, or government agency impersonations common in the region.

It's Time to Get Real

Cyber attackers have gone mobile, gone local, and gone sophisticated. If your training programs haven't caught up, your people are walking into attacks unprepared.

By embracing real-world realism—testing WhatsApp and SMS channels, cloning actual attacks, and adapting simulations to your organization's language and threat landscape—you go beyond awareness. You build readiness.

Because in today's threat environment, phishing awareness isn't enough. Phishing realism is what makes the difference.

LUCY AWARENESS

ITSEC: Cybersecurity Summit 2025 Sponsor

FIVE CONSIDERATIONS FOR SECURING YOUR OT NETWORK

Securing OT networks with a broad set of protections reduces the attack surface and overall risk. It helps maximize operational efficiency and output, enable real-time decision making, and improve worker safety. To select the most effective and comprehensive OT security solution, keep the following in mind:

1. **Network segmentation:** Many OT networks are flat by design, so if a malicious hacker were to get in, they could easily move laterally (east-west) and access all critical systems. Network segmentation blocks unauthorized east-west communication across the network and prevents the spread of malicious traffic; segmentation is a crucial component of basic OT security.

   An OT security solution should offer robust network segmentation capabilities, including network access control (NAC) functionality and the ability to enforce security policies at the individual switch-port level across and within the virtual local area network (VLAN) segments.

   These capabilities protect OT networks and significantly reduce OT security risk.

   ### Questions to ask:

   - How does your solution provide network segmentation capabilities?
   - Do those capabilities extend to each switch port and VLAN?
   - Do those capabilities include NAC functionality?
   - How does your solution automate enforcement?

2. **Visibility and compensating controls:** You can't segment and secure what you can't see. Visibility of assets, vulnerabilities, and threats is a key requirement in basic OT security.

   OT networks are packed with technologies that are not typically found in IT networks, such as industrial automation and control systems, pumps, actuators, furnaces, and conveyor belts. In addition, most of these technologies communicate in clear text protocols that aren't used in IT networks, such as Modbus, Profinet, and DNP3, which can make OT security more complicated.

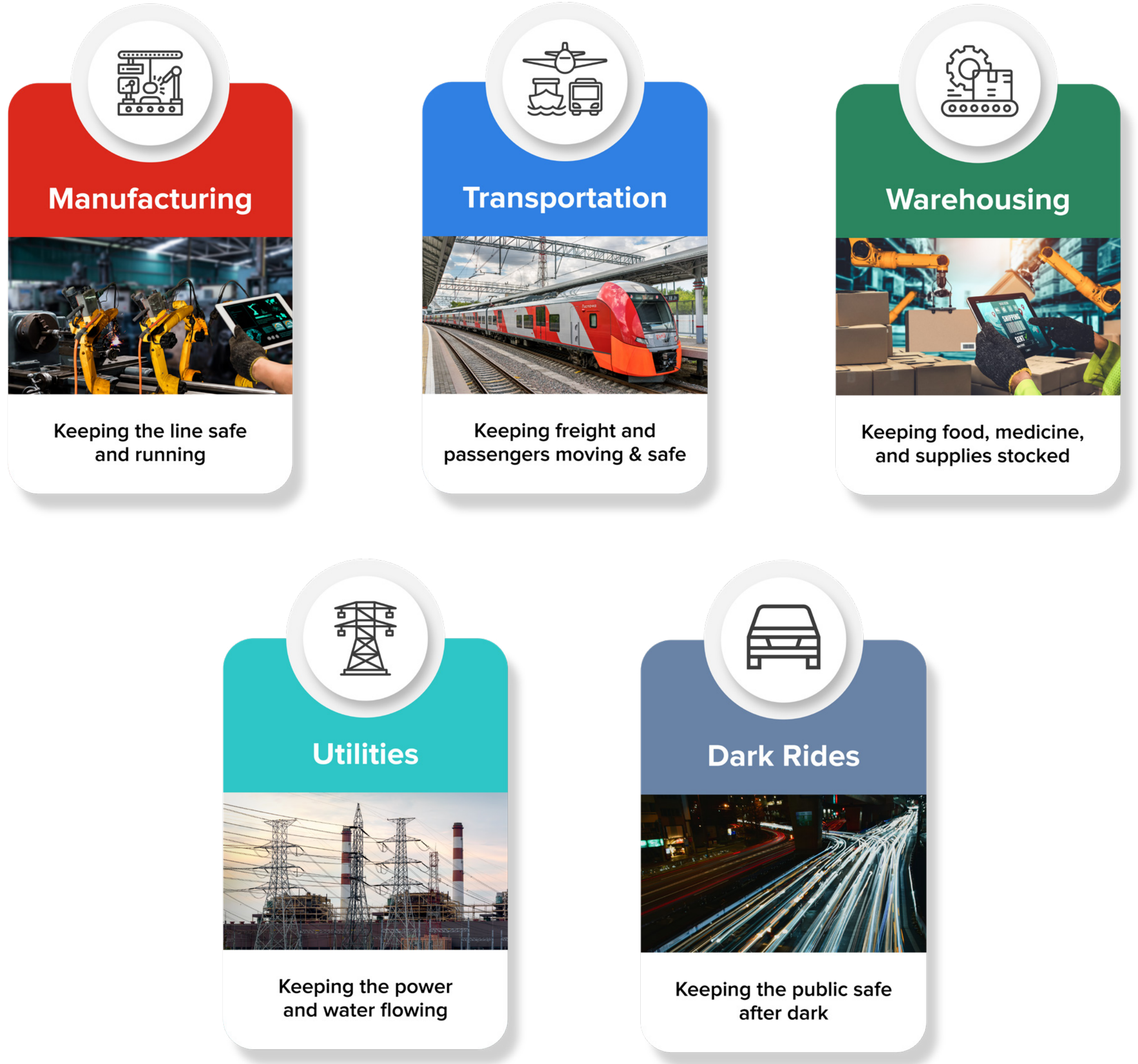
   Many technologies in OT networks are decades old and remain unpatched. Often tied to critical processes such as water pumps or electrical grids, these technologies cannot be shut down for software updates.

   In some cases, vendors of these older devices no longer provide updates. As a result, when OT networks are connected to IT, the internet, and the cloud, the unpatched OT systems are exposed to a wide range of threats, which significantly increases organizational risk.

   An effective OT security solution provides visibility into OT-specific assets, vulnerabilities, and protocols. It also should offer compensating security controls for unpatched systems. Most often, compensating controls come in the form of vulnerability shielding or virtual patching. In this case, an NGFW leverages OT-specific threat intelligence for information regarding OT-specific vulnerabilities and establishes an intrusion prevention system (IPS) rule, which exists in front of those vulnerable systems to prevent attacks. As a result, the legacy OT system can continue operating uninterrupted while also remaining secure.

   ### Questions to ask:

   - How many OT-specific protocols, applications, IPS signatures, and virtual patching rules does your OT security solution support?
   - What compensating controls and enforcement mechanisms can your OT security solution provide for legacy technologies in my OT environment?


Manufacturing
Keeping the line safe and running
Transportation
Keeping freight and passengers moving & safe
Warehousing
Keeping food, medicine, and supplies stocked
Utilities
Keeping the power and water flowing
Dark Rides
Keeping the public safe after dark

3. **SOC and incident response:** Although OT network segmentation and visibility are important, these two strategies alone do not provide complete OT security. As CISOs increasingly take ownership of OT infrastructure, they need to show meaningful reductions in the mean time to detect (MTTD) and mean time to respond (MTTR) to cyberthreats as part of a larger effort to reduce organizational risk.

   OT networks should be included in corporate SOC and incident response plans. By incorporating OT infrastructure into these business areas, organizations can begin to converge IT and OT and simplify cybersecurity management. With the ability to detect and respond to threats wherever they occur, CISOs and their teams can drastically reduce the impact of a breach and stop attacks from spreading into more sensitive areas of the OT environment.

   Tools such as network detection and response, endpoint detection and response, deception technologies, and OT-focused central management and reporting can all make the CISO's job easier and make the effort to secure OT more effective. These solutions can also help CISOs on their journey to assess their adherence to often complex regulatory compliance standards.

Questions to ask:

- What advanced cybersecurity capabilities does your OT security solution offer?
- How does your OT security solution enable me to visualize threats and make assessments?

4. **Platform Approach:** Many organizations acquire various security solutions from different vendors to address rapidly evolving OT threats and the expanding attack surface. Having a collection of disparate solutions often results in an overly complex security architecture that can inhibit visibility while increasing the burden on already limited security teams.A platform-based approach to security can help organizations consolidate vendors and simplify their architecture. A robust security platform with specific capabilities for IT networks and OT environments can simplify solution integration, improve security, and enable centralized management for enhanced efficiency. Integration can also provide a foundation for automated threat response.

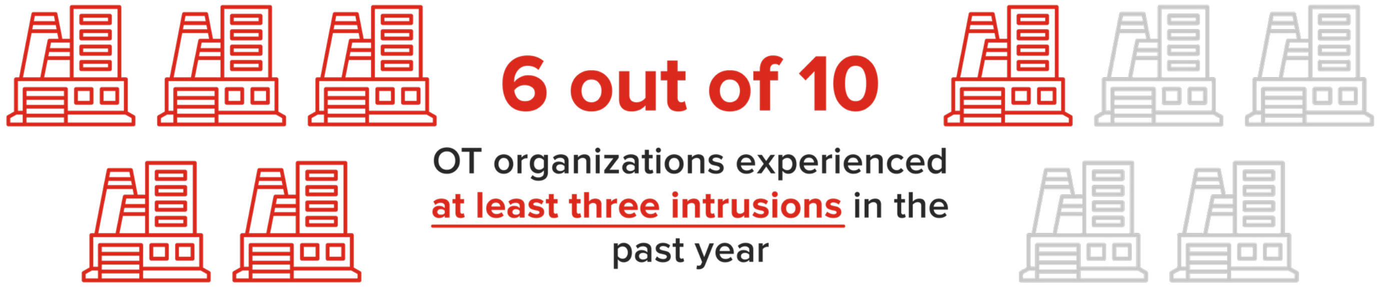
Questions to ask:

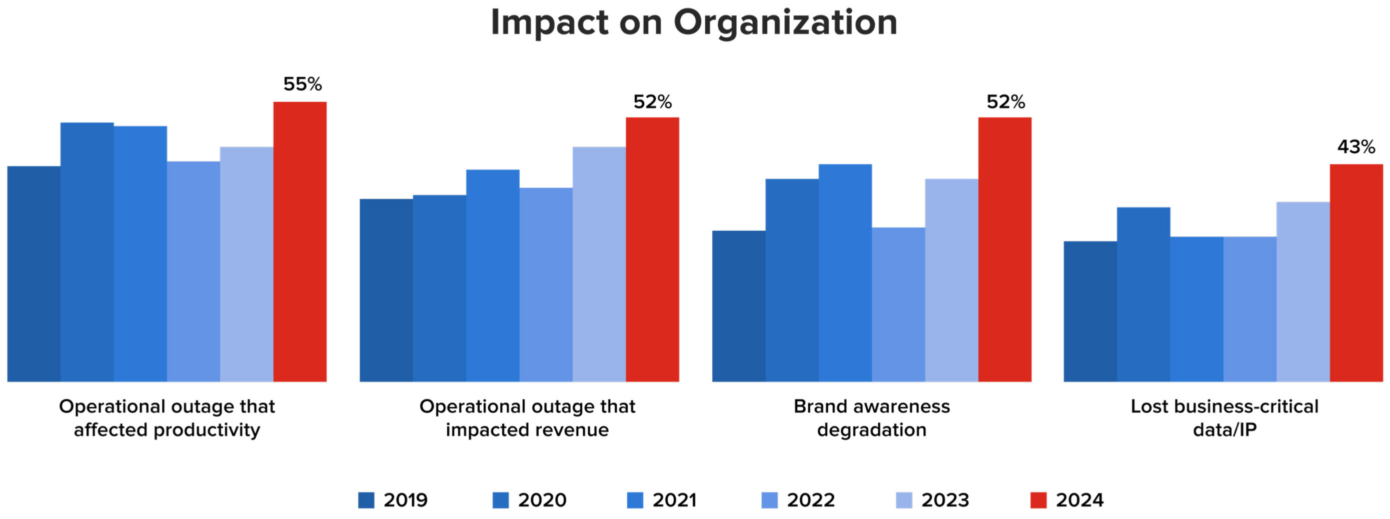
- What capabilities does your cybersecurity platform include?
- Can I manage and automate those capabilities with a single management console?
- Which third-party integration partners does your cybersecurity platform support?

5. **OT threat intelligence:** OT security depends on timely awareness and precise analytical insights about imminent risks. A platform-based security architecture integrates threat intelligence for near-real-time protection against the latest threats, attack variants, and exposures. Although many OT security breaches originate through IT-targeted cyberattacks that spread laterally, some of the most significant incidents over the past 15 years were generated through malware explicitly crafted to exploit OT technologies. Organizations should ensure their threat intelligence and content sources include robust, OT-specific information in their threat feeds and threat-intel services.

Questions to ask:

- What is the scope of threat intelligence backing your security product or solution?
- How many OT protocols, applications, IPS signatures, and virtual patching or shielding rules are included?





FROM REACTIVE TO AUTONOMOUS:

How Agentic AI is Revolutionizing the Modern-Day SOC Operations

Sophisticated cyber threats continue to rise, and the stakes in cybersecurity are escalating at an unprecedented pace in today's hyperconnected digital landscape. Advanced technologies, intense geopolitical tensions, a widening cyber skills gap, and increasing vulnerabilities in the supply chain are some of the challenges faced by Security Operations Centers (SOCs), the nerve centers of an organization's cyber defense. Unfortunately, the strain on SOC operations runs even deeper.

Alert Fatigue and Data Overload are Drowning SOCs

Cyberattacks continue to penetrate SOC defenses with innovative tactics, while security teams face a flood of security alerts and the explosion of log data daily. Analysts are already stretched beyond capacity and are now further overwhelmed by high alert volumes and false positives, as they lack access to alert context. They are also exhausted by duplicated work, navigating the alert-centric SOC model, with alert fatigue setting in amidst the constant storm of noise and alerts. According to the SANS 2024 Detection and Response Survey, 66% of SOC teams can't keep pace with alerts, and 70% of junior analysts leave within three years.

Waning Relevance of Traditional SIEMs

Security Information and Event Management (SIEM) systems are crucial tools that provide technological support and augment the capabilities of SOC teams. For several years, traditional SIEMs have served as a key feature in enterprise cybersecurity. Relying on pre-defined logic and case-based correlated rules, they aid enterprises in detecting known threats and anomalies, an adequate approach when cyberattacks follow a predictable pattern with the infrastructure primarily on-premises.

However, traditional SIEMs are plagued with scalability issues and lack the intelligence and analytical capabilities required to address modern-day threats.

Transitioning Toward An Autonomous SOC

The existential security challenges seen with traditional SIEMs cannot be fixed with manual tuning. The answer lies in reimagining the SOC with modular Agentic AI that drive autonomous operations.

- **Extracts and refines content from natural language**

  By leveraging natural language processing, agentic AI can convert natural language security objectives into detection rules that can be autonomously deployed. The SOC analyst's intent is transformed into high-precision detection content at speed. To ensure detections are precise, simulations of various attack scenarios are run, issues are flagged to help analysts craft and fine-tune threat detection logic.

- **Suppresses false positives**

  False positives are poorly managed with traditional SIEM. draining the time and resources of the SOC, and compromising the overall effectiveness of the security teams. On the other hand, agentic AI suppresses false positives and reduce alert fatigue so analysts can focus on real threats. This is done by leveraging LLM reasoning, behavioral patterns, and feedback from analysts, where irrelevant alerts that derail security operations are classified, deduplicated, and suppressed.

- **Enables the shift from rule-bound triggers to risk-based response**

  Reactive SOCs rely on rule-based systems that use pre-defined logic where alerts are triggered based on patterns or known signatures, not adaptable for the dynamic environments of the digital age. Agentic AI, on the other hand, prioritize proactive defense by identifying emerging risks and facilitating automated incident response. Alerts are managed in real-time, minimizing downtime and costs while risk-optimizing the organization's security posture.

- **Spots insider threats before they escalate into incidents**

  Individuals within organizations can misuse their access to the company's resources unintentionally or with malicious intent and detecting these insider threats remains a significant challenge. Agentic AI assists by detecting early indicators of insider threats through psycholinguistic analysis, behavioral drift, and contextual risk while flagging risky behavior related to insider threats. The agents build adaptive profiles enabling SOC teams to proactively act on emerging risks before any damage occurs.

- **Curates rich threat context, cutting investigation time**

  With cyber threats evolving constantly, the relevant context plays a key role. Agentic AI uses the knowledge repository to understand the context and the connections between various fragments of information. The agents compile investigation findings, enrich them with contextual details, and present clear natural language summaries autonomously, enabling analysts to quickly grasp both the severity and context of each case.

The transition from reactive to autonomous SOC operations marks a significant shift in cybersecurity. Agentic AI represents the future of security operations - intelligent, explainable, and built to scale.

ITSEC CYBERSECURITY SUMMIT 2025
The Largest Critical Infrastructure Cybersecurity
Event in Southeast Asia

SPECIAL THANKS TO

SPONSOR

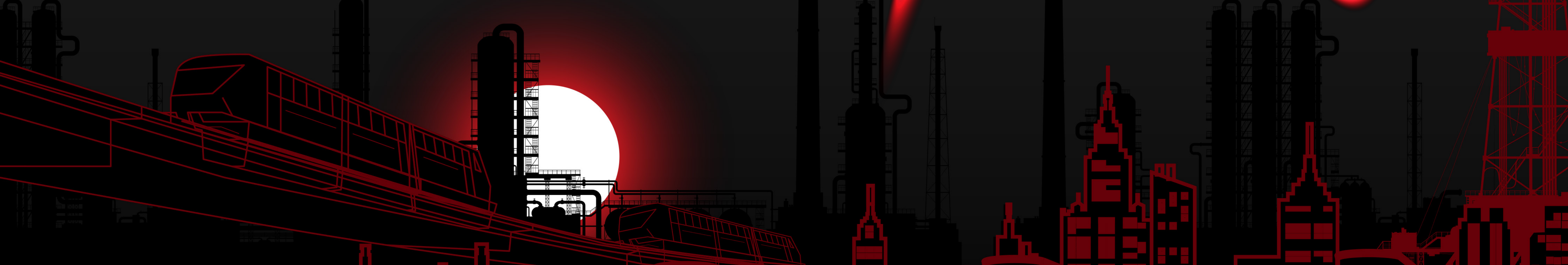
aikido
BLACKDUCK
FORTINET
Google Cloud
LUCY AWARENESS
mimecast
PROMON
securonix
segura
SOCRadar
vicarius

MEDIA PARTNERS

Akurat.co
BERITA SATU
BTV
CNN Indonesia
HEAPTALK
inilah.com
INVESTOR.ID
JAKARTAGLOBE.ID
KOMPAS.com
LIPUTAN 6
MEDIA INDONESIA
merdeka.com
sonora Jakarta 92.0 FM
smartfm Jakarta 95.9 FM
TheJakartaPost
TIMES INDONESIA

SEE YOU AT

ITSEC: CYBERSECURITY SUMMIT 2026



ITSEC™

SECURITY DELIVERED

PT. ITSEC Asia
Noble House, Level 11
jakarta, Indonesia 12950

☎ +62 (21) 29783050

✉ contact@itsecasia.com

itsec.asia