



Philippine Threat Landscape Report 2024-2025

December 2024



TABLE OF CONTENTS

Overview	3
Methodology	4
Overview of Emerging Cyber Threats in 2024	5
Social Engineering	5
Malware	5
Social media Impersonations	5
Distributed Denial-of-Service (DDoS)	6
Supply Chain Attacks	6
Vulnerabilities and Exploits	6
Deeper Look into the Cyber Threats for the Philippine Threat Landscape 2024	7
Malware	7
Vulnerabilities	10
Social Engineering	12
Brand	17
Data Exposure	18
Attackware	20
Supply Chain	26
Staying Ahead of the Curve: Evolving Cyber Threats and Strategic Priorities in 2025	27
Contact us	29
About Cyberint	29

OVERVIEW

The Cyberint (now a Check Point Company) Philippine Threat Landscape 2024-2025 report unravels the evolving cyber threats and scam operations targeting organizations in the Philippines—mainly within the Government, Education, Financial, and Telecommunications sectors.

Data from Cyberint sources indicates a surge in cyber threats such as malware, social engineering, and system exploitations. This increase is driven by political and sociological ideologies, global conflicts, technological shifts, and local scam operations, particularly involving Philippine hacktivists.

In 2024, malware infections, especially InfoStealers, continue to rise, exposing sensitive information like confidential files and credentials. Philippine-based threat actors and scam operators use advanced techniques to conduct phishing campaigns, impersonating local organizations—from government to telecommunication sectors—to target financial industry customers.

Meanwhile, DDoS attacks have become a trend in the Philippines. It began during the “April Lulz” event, a campaign celebrated by local threat actors annually, where they actively conduct cyber attacks targeting local entities for the whole month of April. Amidst the numerous cyber attacks, it's encouraging to note that we reported a significant decline in ransomware attacks targeting the Philippines.



METHODOLOGY

Cyberint's Philippine Threat Landscape Report 2024-2025 employs a comprehensive intelligence strategy that combines both proprietary and public data sources. Our intelligence is gathered from Cyberint and Check Point sources, that track a variety of threat vectors using modules like Attack Surface Management, Darkweb Threat Intelligence, Supply Chain Intelligence, Malware Intelligence, Phishing Detection, Social Media Monitoring, and more.

Cyberint, now a Check Point Company delivers essential alerts and indicators that shape our analysis, enabling us to present an intelligence-driven overview of the cyber security threat landscape in the Philippines. The information in this report is based on a sample of around 127,000 intelligence alerts collected from December 1, 2021, to December 1, 2024, from around 15 companies across various industries in the Philippines.

Critical Alerts by Industry (December 2021-2024) in the Philippines



Banking and
Financial Services

66%



Media and
Entertainment

11%



Technology
and IT

8%



Real
Estate

6%



Retail and
Consumer Goods

5%



Healthcare

2%



Energy and
Industrial

1%



Hospitality

0.6%



Shared Services

0.4%

We also utilize open-source intelligence (OSINT) by incorporating threat feeds, news articles, and research publications from cyber security professionals and regulatory authorities.

OVERVIEW OF EMERGING CYBER THREATS IN 2024

SOCIAL ENGINEERING

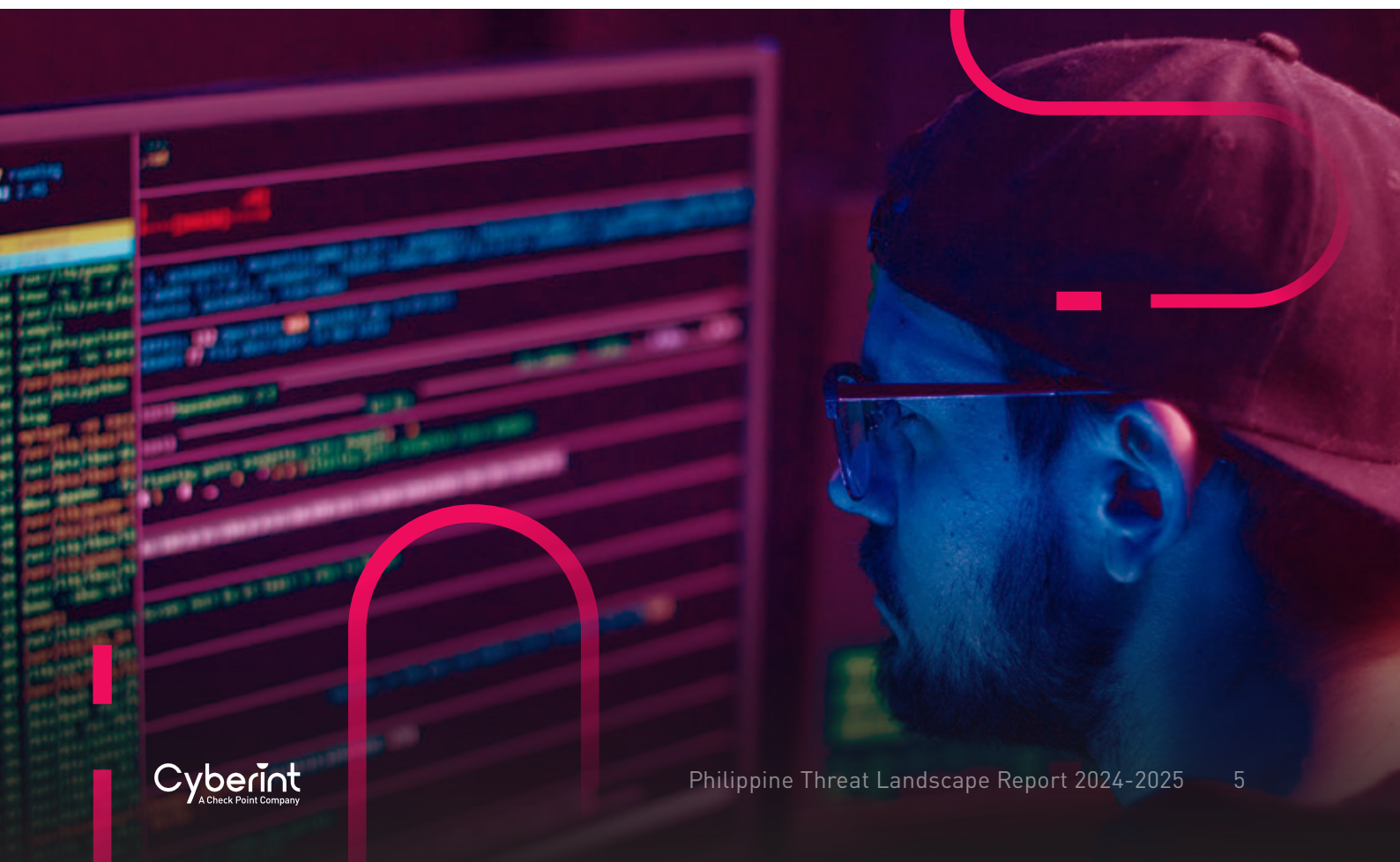
Social Engineering remains a highly effective attack vector in the Philippine threat landscape. Local threat actors continue to operate Phishing campaigns, where some of them leverage new techniques to lure more users into falling into their fraudulent schemes.

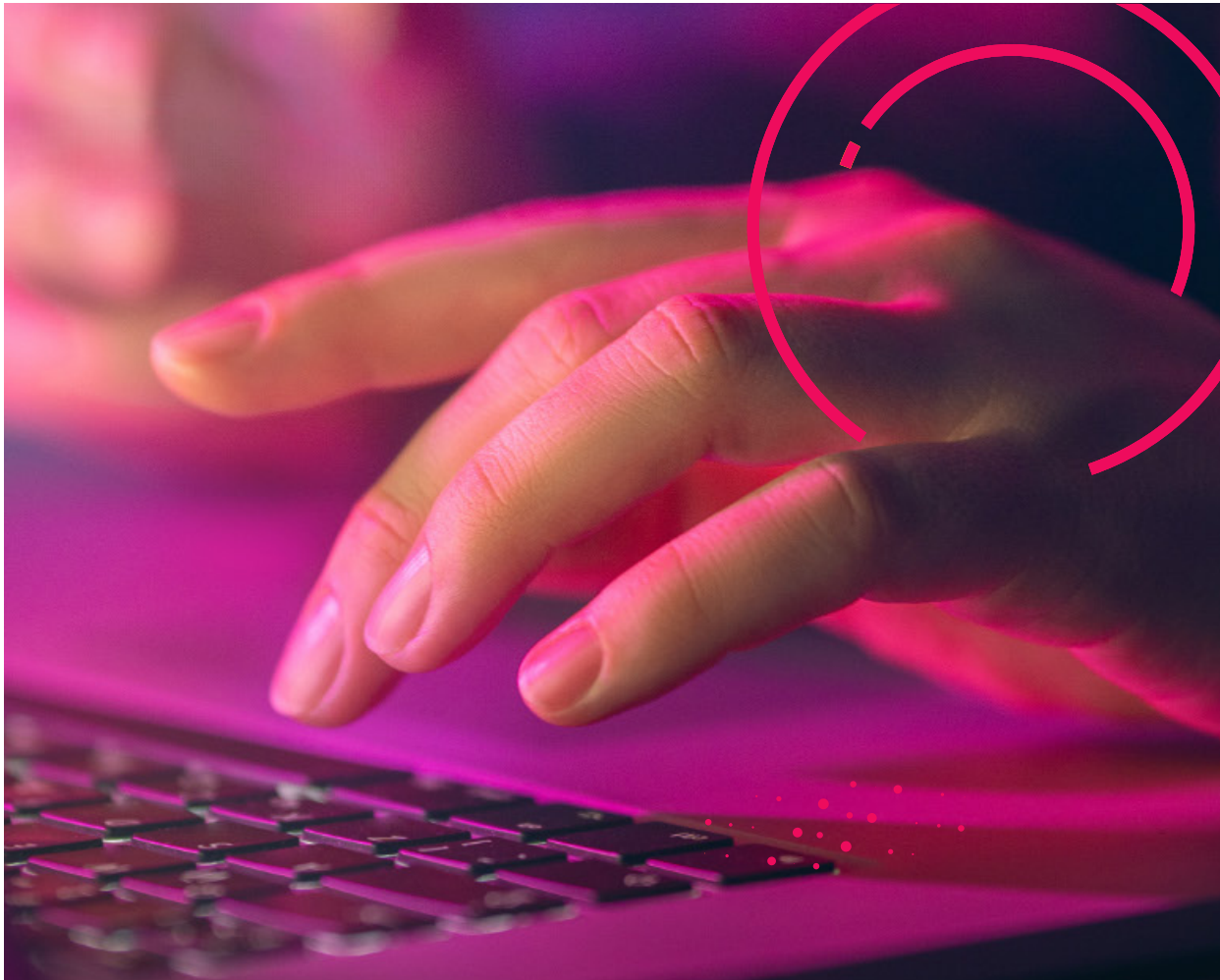
MALWARE

Malware remains the top cyber threat in the Philippine threat landscape, considering its broad category, including trojans, worms, spyware, and viruses. Based on Cyberint sources, we have observed a continuous trend in Malware-as-a-Service (MaaS) being offered in the dark web, which allows even some inept threat actors to deploy sophisticated malware.

SOCIAL MEDIA IMPERSONATIONS

Impersonations are everywhere! Threat actors nowadays can easily impersonate organizations, including high-ranking officials, through social media platforms. By effectively impersonating a known entity, threat actors can initiate a scam operation targeting company employees and customers.





DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

Newly discovered local threat actors are now conducting Distributed Denial-of-Service (DDoS) attacks, mainly targeting financial, government, media, and educational institutions. Some are already offering DDoS tools in the underground, making it easier, even for unskilled threat actors, to conduct their own DDoS campaign.

SUPPLY CHAIN ATTACKS

Supply Chain attacks continue to increase in 2024. As Philippine-based organizations leverage new technologies and services, risks for data exposure due to supply chain incidents will rise.

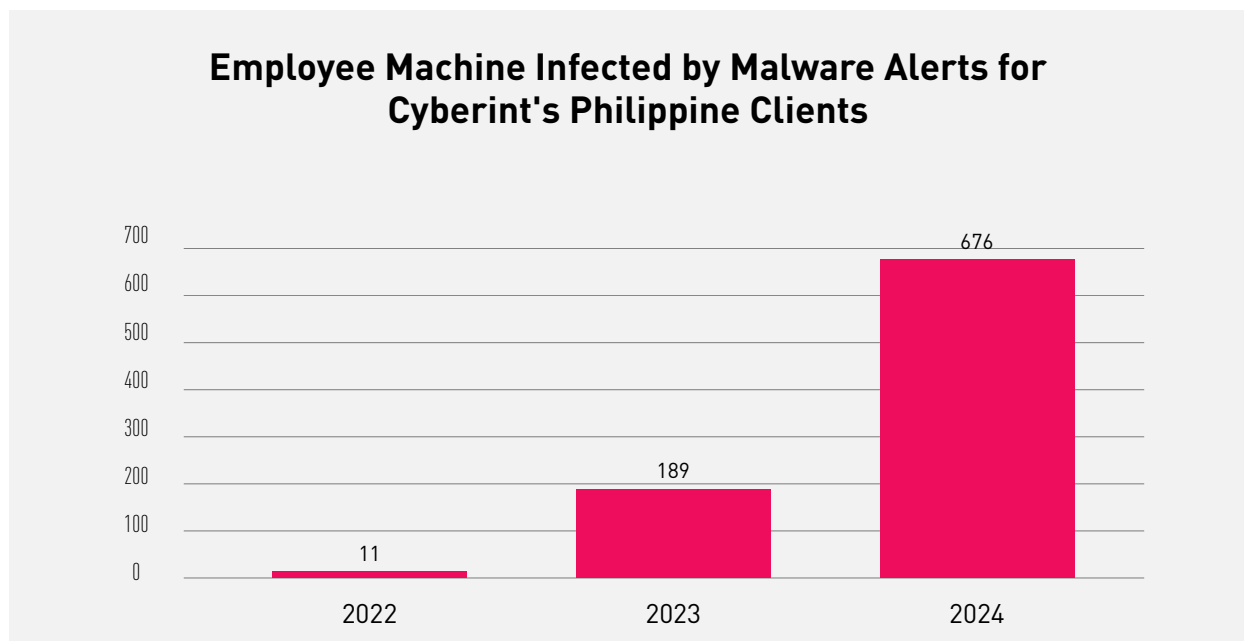
VULNERABILITIES AND EXPLOITS

The race between vulnerabilities and threat actors has been constant in 2024 and will persist in 2025. With more innovations every year, we can expect a continuous curve for vulnerabilities, thus giving more exploitation vectors for threat actors to gain a foothold in targeted organizations.

DEEPER LOOK INTO THE CYBER THREATS FOR THE PHILIPPINE THREAT LANDSCAPE 2024

MALWARE

As we continue to enhance our sources and services, more malware infections for our clients' employee machines have been discovered. The majority of these malware infections came from the personal devices of clients' employees, which were utilized for work-related activities.



INFOSTEALERS

In the Philippines, Information Stealers (a.k.a. Infostealers), a type of malware that can exfiltrate sensitive information (i.e., browser credentials, cookies, cache, crypto wallets, desktop files, etc.), became the gateway for threat actors to easily gain unauthorized access to insecure portals, resulting in exposure of sensitive information. Nowadays, Infostealer logs are scattered across the dark web, making it easier for threat actors to source exposed credentials of their targeted entity.

Infostealers became more effective against Philippine-based organizations' employees during and after the COVID-19 pandemic due to the adjustments made by the Philippine government. In contrast, most local companies are now allowing work-from-home setups.

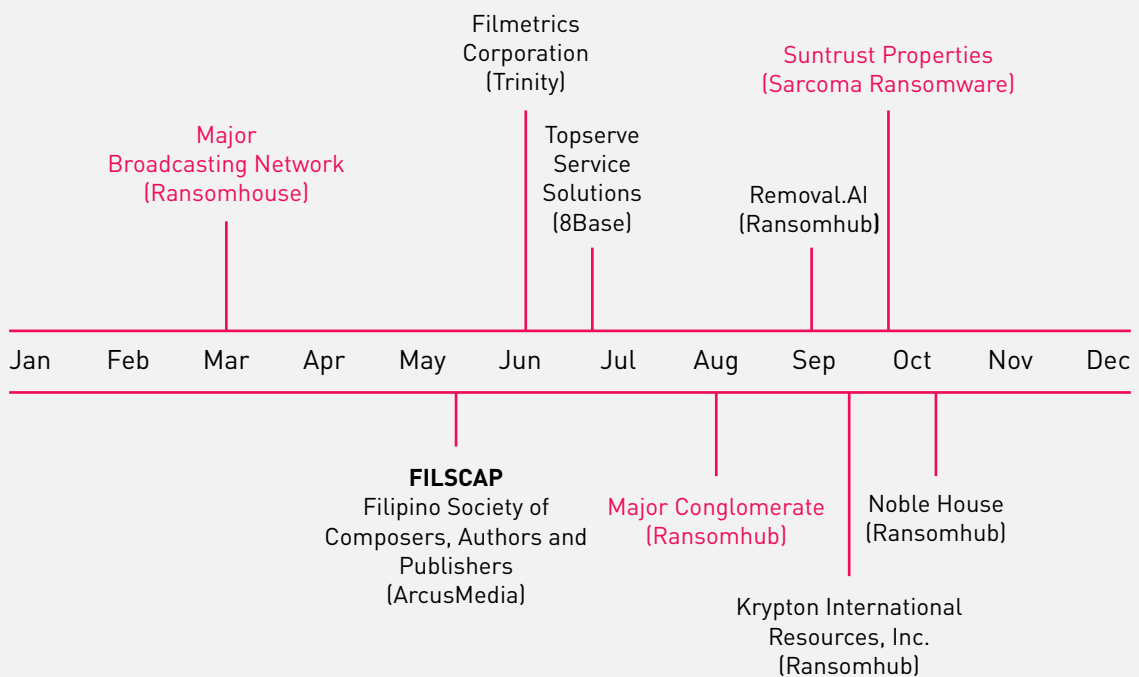
Based on Cyberint (now a Check Point Company) sources, many Filipinos who work from home are more susceptible to violating an organization's information security policies. We have observed a massive number of Filipino employees who use their personal devices (i.e., desktops, laptops, etc.) to access work-related portals, thus amplifying the risks of having credentials exposure whenever these personal devices get infected by Infostealers.



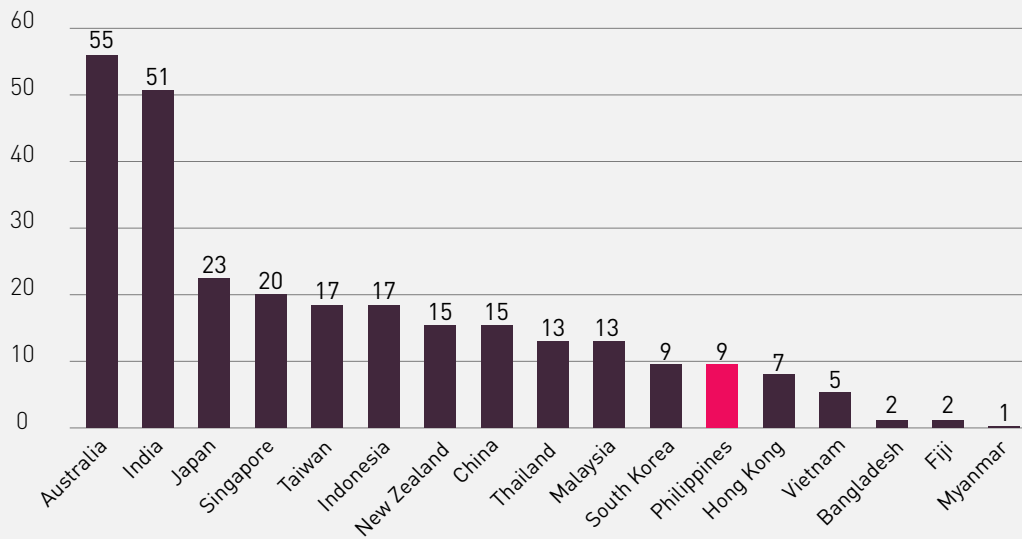
RANSOMWARE

Ransomware continues to be one of the most critical threats, not only in the Philippines but around the globe. However, we have observed a decrease in ransomware attacks targeting the Philippines in 2024 compared to 2023.

Ransomware Attacks 2024 Timeline in the Philippines



Philippines Ranked 12th in Ransomware Attacks across APAC



PH Ransomware 2023 2024

2023

2024

20

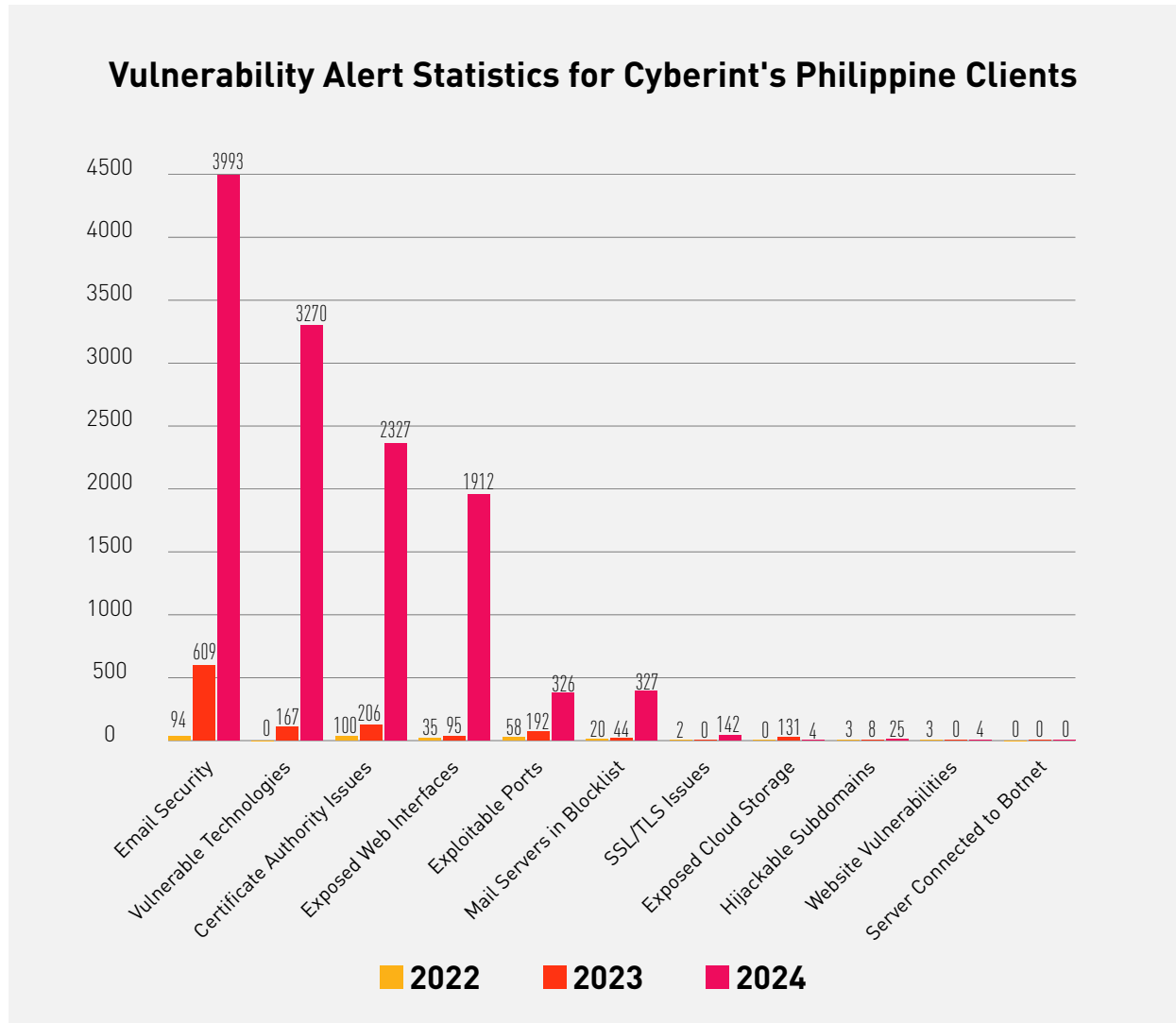
9

The **Philippines** will likely not be targeted as much as developed countries in 2024.

The motives of the majority of Local Threat Actors will still stay the same:
Hacktivism, Ideology, and Personal Satisfaction.

Ransomware is still not in the plans of local threat actors.

VULNERABILITIES



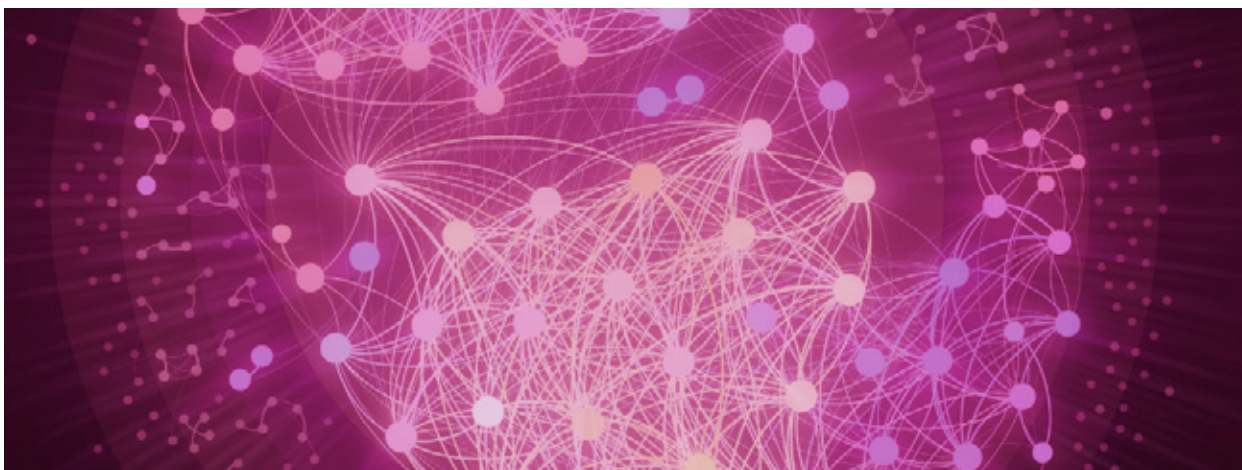
Cyberint observed a rise in most vulnerability exposure items for our Philippine clients in 2024 compared to past years. Several factors for this increase include new clients, more Attack Surface Management assets (i.e., domains, subdomains, and IP addresses)—added or discovered for monitoring—for each client, new vulnerabilities affecting our clients’ assets and technologies, and improvements in Cyberint’s Attack Surface Monitoring module for a better external risk management service.

Cyberint Attack Surface Management

Cyberint Attack Surface Monitoring & Management provides automatic and full visibility into your digital presence – uncovering security issues and vulnerabilities that potential adversaries can exploit.

- Exploitable Ports:** Cyberint monitors open network entry points that, if exploited, can lead to significant security breaches, allowing threat actors to install malware, exfiltrate sensitive data, or disrupt business operations.

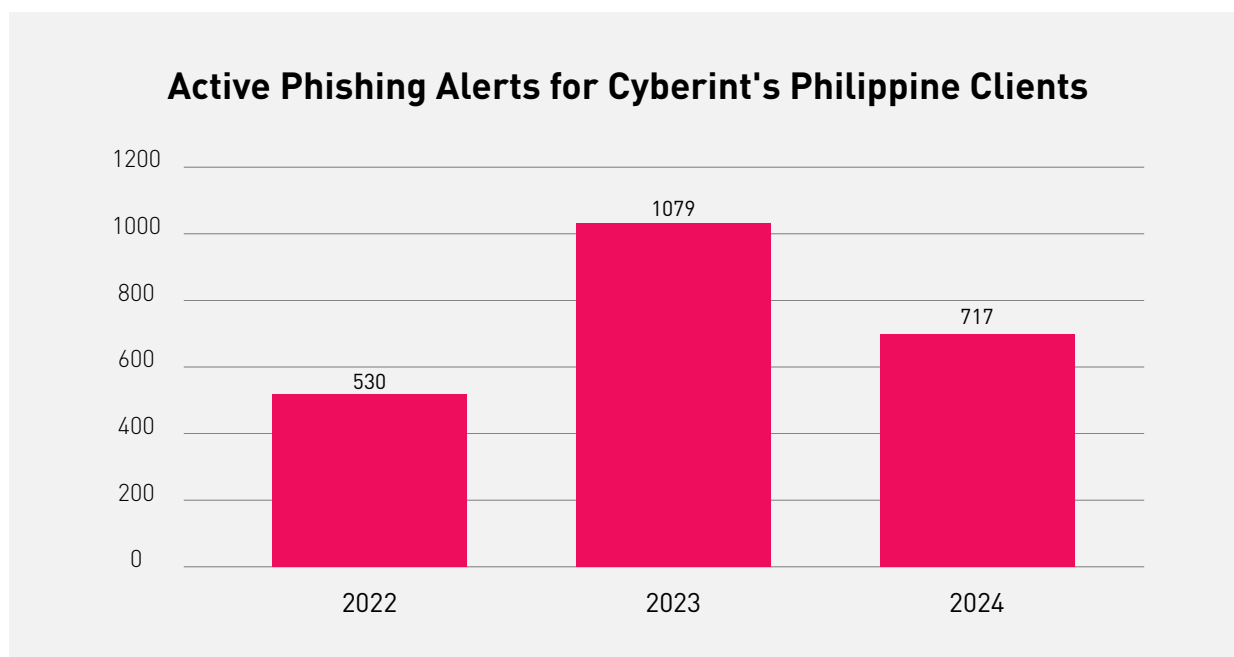
- **Certificate Authority Issues:** Misconfigured or compromised certificate authorities can result in man-in-the-middle attacks, significantly weakening a company's ability to maintain secure communications.
- **Email Security:** The absence or misconfiguration of SPF and DMARC records, among other factors, leaves companies vulnerable to email spoofing and phishing attacks.
- **Vulnerable Technologies:** Outdated software with known vulnerabilities (e.g., old versions of NGINX or JavaScript) can be easily exploited, putting sensitive systems and data at risk.
- **Exposed Web Interfaces:** Public-facing login pages or interfaces that are meant to be internal can provide attackers with direct access to sensitive systems, heightening the risk of breaches.
- **Hijackable Subdomains:** Hijackable subdomains enable attackers to impersonate trusted sections of a company's website, making it easier to conduct phishing attacks or distribute malware.
- **Mail Servers in Blocklist:** Blocklisted mail servers lead to email delivery problems, disrupt communication with clients and partners, and harm the company's reputation.
- **Website Vulnerabilities:** Vulnerabilities like cross-site scripting (XSS) enable attackers to insert harmful scripts, which can result in data theft or compromise user security.
- **SSL/TLS Issues:** Outdated or weak SSL/TLS configurations can leave encrypted communications vulnerable, enabling attackers to intercept sensitive data or breach user privacy.
- **Exposed Cloud Storage:** Cloud storage buckets that are publicly accessible can result in unauthorized data access, risking confidential company or client information.
- **Server Connected to Botnet:** Servers compromised by botnet malware can be exploited for malicious activities, resulting in reputational damage, data loss, and possible legal consequences.



SOCIAL ENGINEERING

In terms of social engineering techniques, phishing operations are rampant in the Philippines, mainly targeting the financial sector. In 2024, a decrease in phishing alerts targeting Cyberint's clients was observed compared to 2023. Cyberint, now a Check Point Company believes that this decline in typical local Phishing operations is due to new techniques being explored by threat actors in preparation for 2025. In contrast, we have observed an increase in social engineering campaigns leveraging social media advertisements (ads) and impersonating pages.

PHISHING



Phishing operations in the Philippines have evolved significantly, with a dramatic surge in both sophistication and frequency. Over the past few years, local threat actors have been looking for new ways to conduct phishing operations.

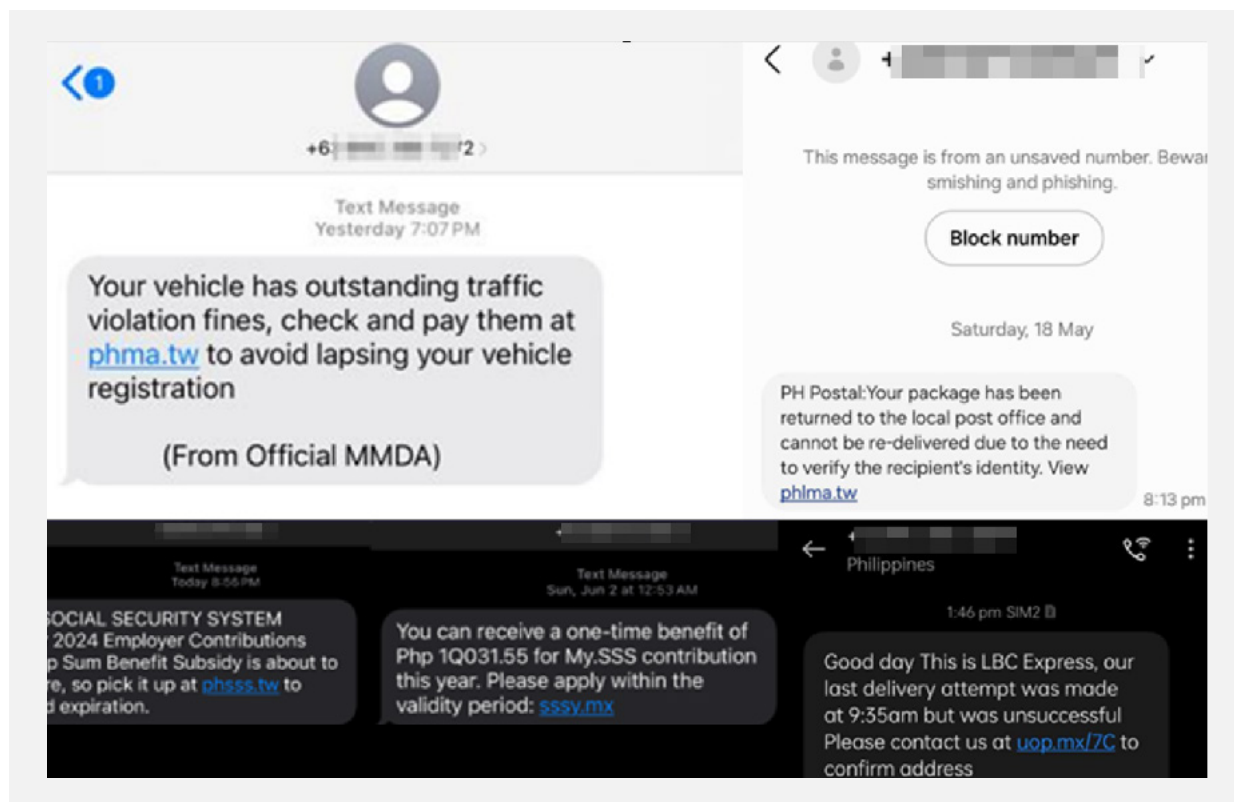
They started with the traditional phishing techniques and shifted to a more sophisticated one known as True Login Phishing, where they automate the exfiltration of credentials and OTPs by abusing insecure APIs or any vulnerabilities from an online service, such as online or mobile banking applications.

Cyber criminals have become more adept at exploiting digital communication channels, often tricking individuals into providing sensitive information through fake websites, promotions, or app downloads.

Despite efforts like the SIM Card Registration Law, which aims to trace scammers more effectively, these threats persist, highlighting the need for enhanced cyber security measures and public awareness.

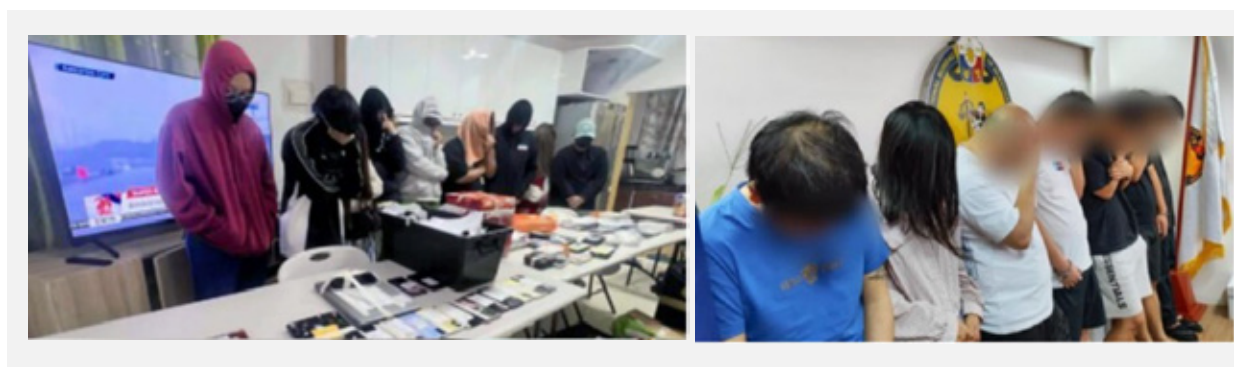
SMISHING

In 2024, Smishing—Phishing via SMS—took the spotlight in the Philippine threat landscape. During the 1st quarter of the year, a Smishing campaign began operating. This campaign initially impersonated government and logistics organizations, such as the Land Transportation Office (LTO), Social Security System (SSS), PHLPost, and more.



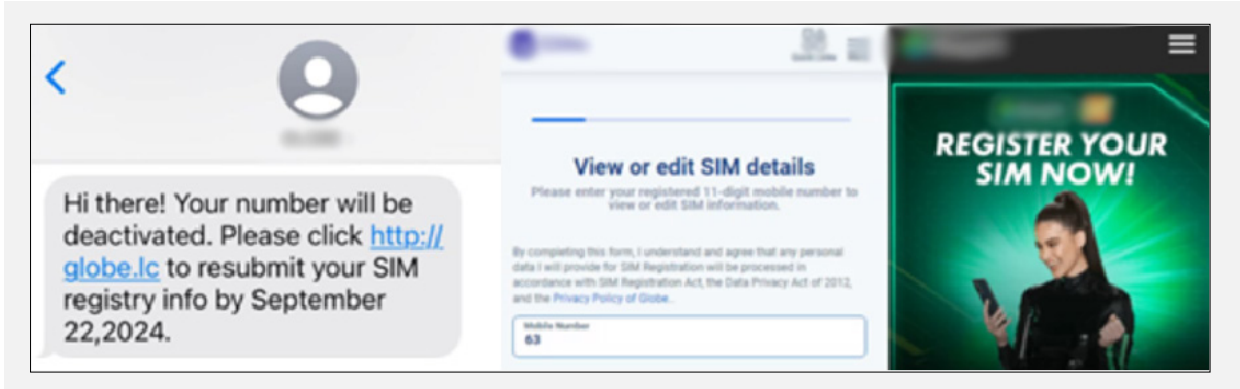
Samples of Smishing Messages Impersonating Government and Logistics Organizations

Over the past months, multiple local scam hubs were consecutively infiltrated by the National Bureau of Investigation (NBI), resulting in the arrest of several Chinese and Filipino nationals who mainly conduct scam operations, including Phishing targeting local banks' customers.



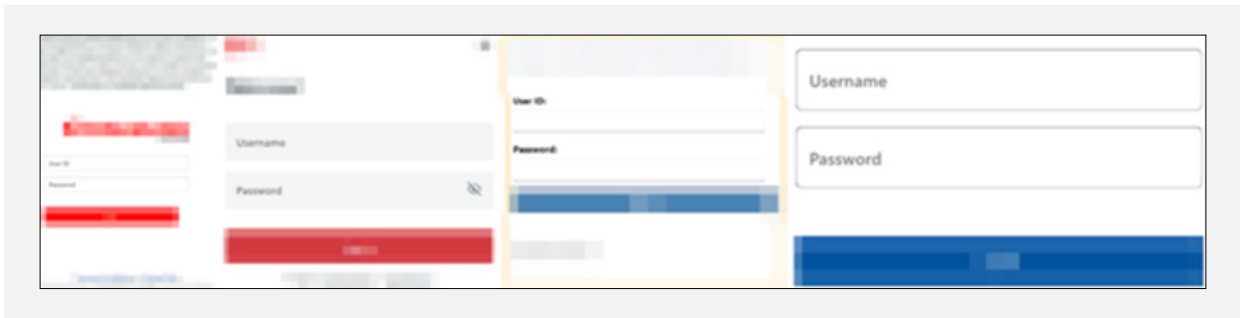
Apprehensions of Local Scam Operators

As per Cyberint, now a Check Point Company's observation, these successive apprehensions have led to an abrupt interruption of the smishing campaign around September 2024. However, in October 2024, the campaign returned with a new theme—this time impersonating telecommunications companies, luring the users into believing a fake deactivation of SIM card notification and tricking users into reprocessing their SIM card registration by clicking the Phishing link.

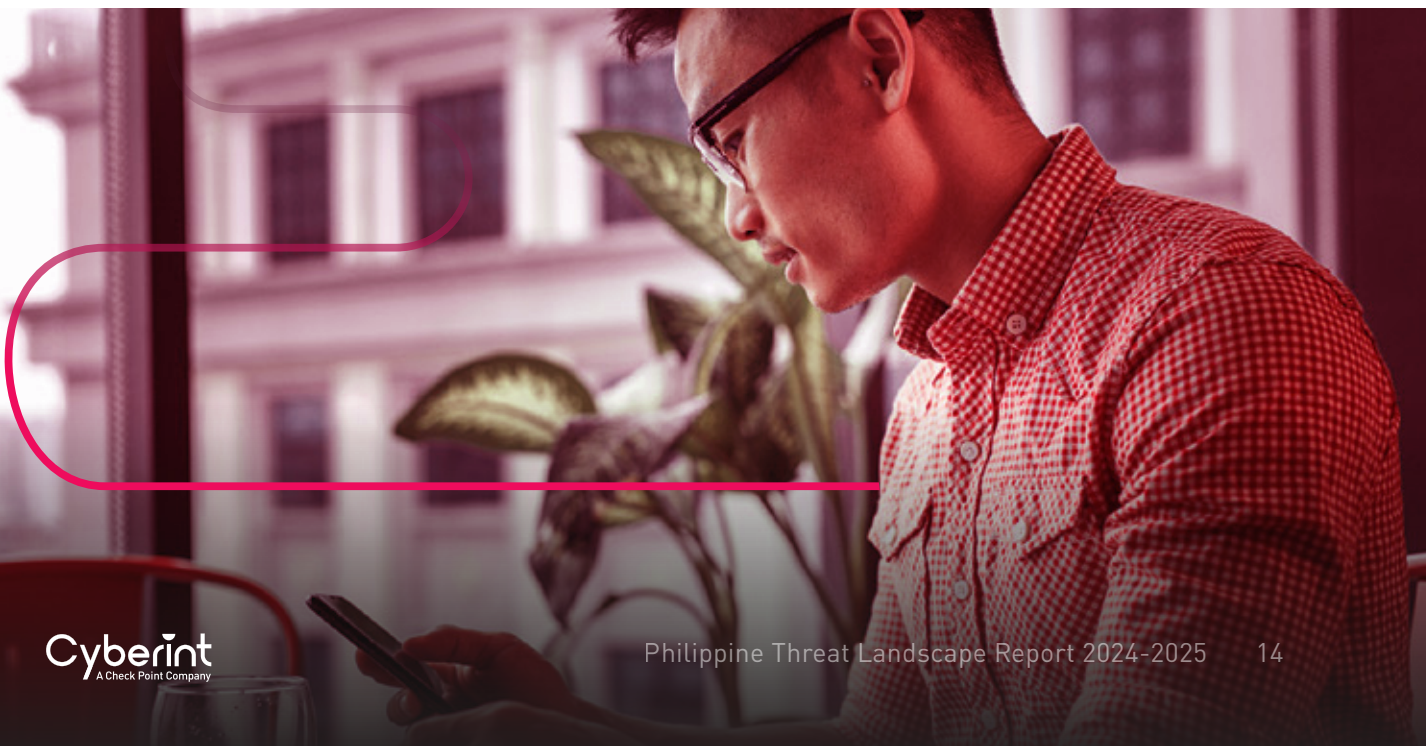


Samples of Smishing Messages Impersonating Telecommunications Companies

The main goal of this smishing campaign is to steal the online banking credentials of victims by impersonating online banking pages as their final landing pages.



Samples of Phishing Pages Impersonating Philippine-based Online Banking Portals

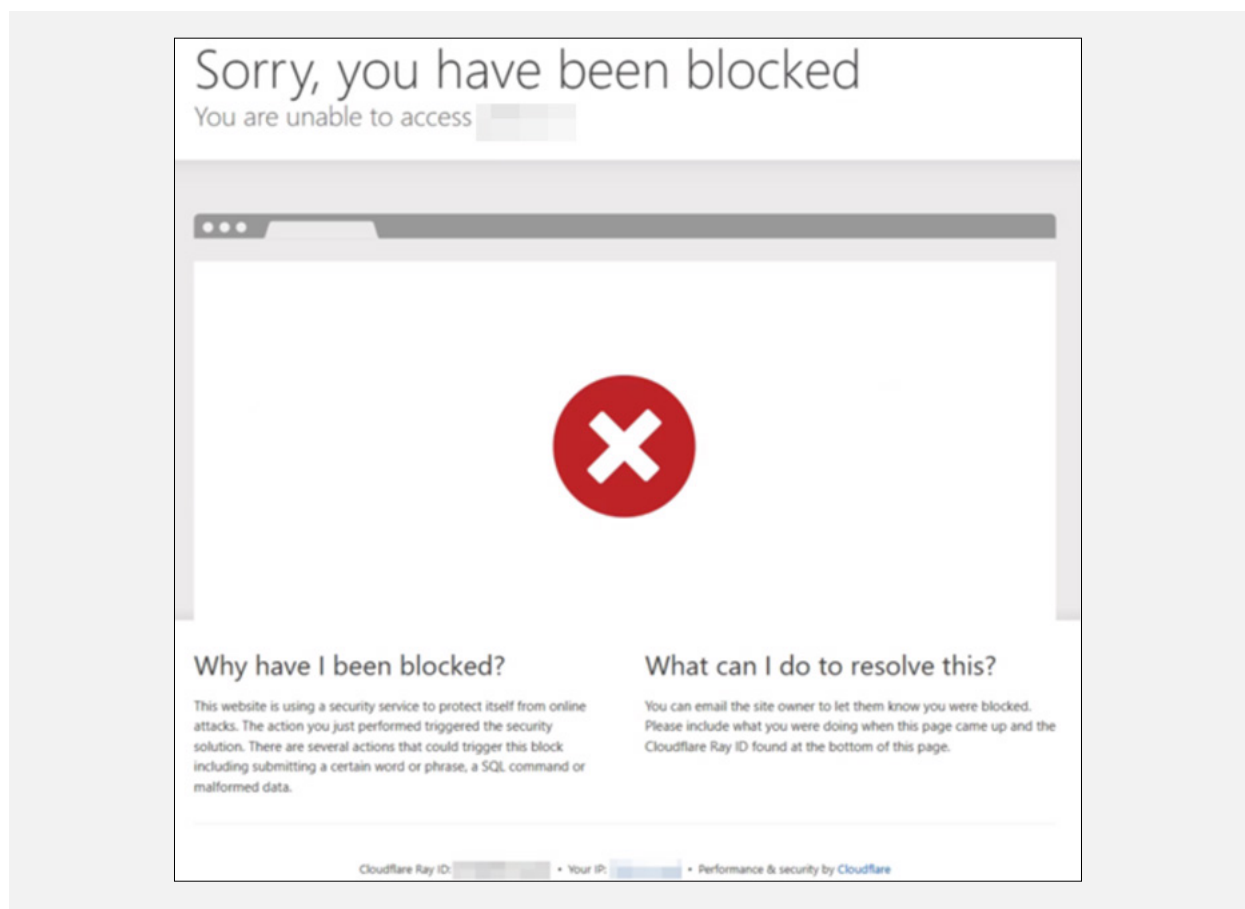




DEVICE AND GEO FILTERING MECHANISMS

The latest local phishing operations leverage techniques that threat actors are utilizing in targeting well-developed countries, like the United States of America and the European region.

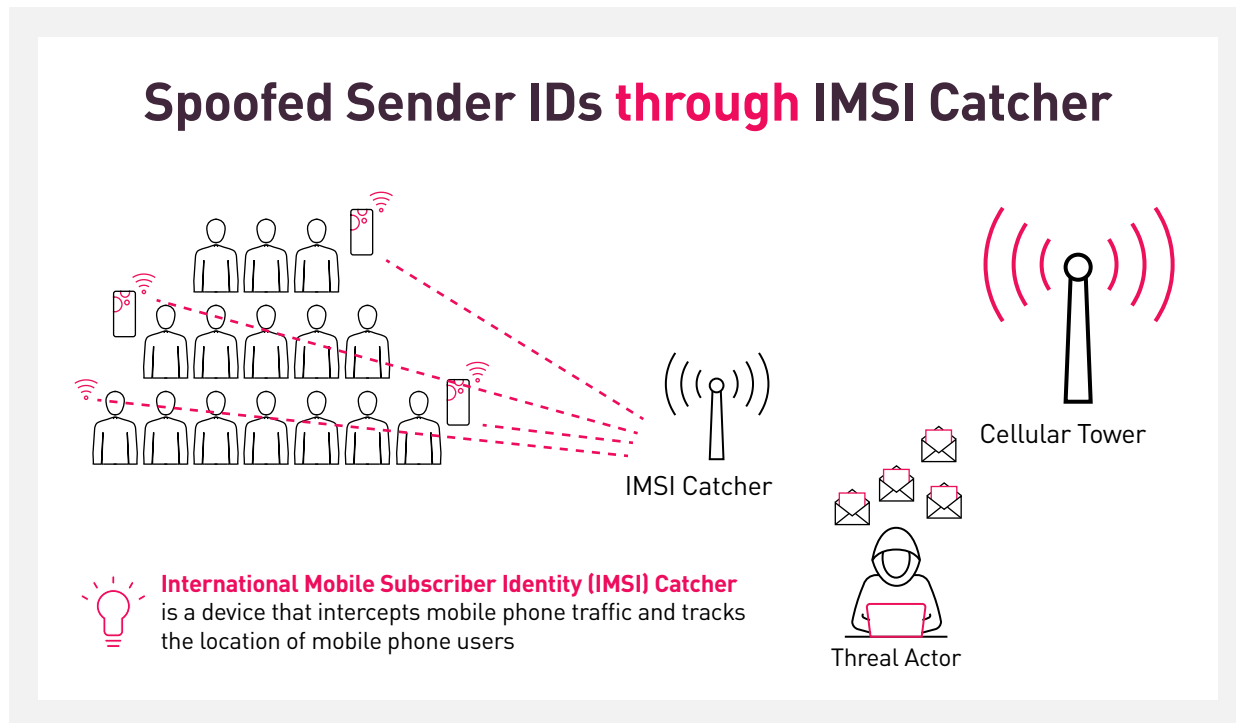
This technique is known as Device and Geo Filtering, which recent threat actors apply to hosted phishing domains to ensure that they will only be accessible when visited from a Philippine-based IP address using a mobile device. Thus, enhancing their defense mechanism to evade detection through sandbox and other security controls.



Device and Geo Filtering via Cloudflare used in the Recent Smishing Domains

SMISHING VIA IMSI-CATCHER DEVICES

A device for intercepting mobile phone traffic leveraged in well-developed countries like the United States—known as **IMSI (International Mobile Subscriber Identity) Catcher**, also known as **Cell-Site Simulators** or **Stingrays**—is being leveraged by Smishing operators targeting Filipinos in 2024.



Visualization for IMSI-Catchers Intercepting Mobile Network Traffics

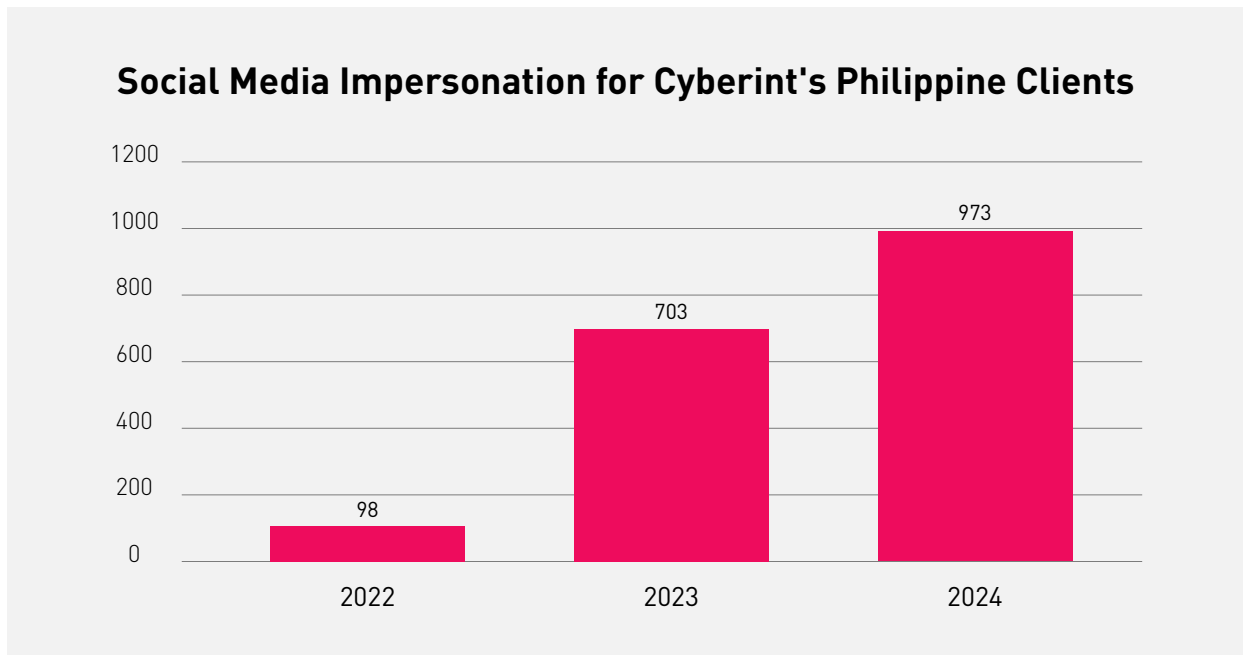
The local Smishing campaign leveraging IMSI-Catcher devices was highly observed during the November 1 and 2 holidays—**All Saints and Souls' Day** (a.k.a. **Undas**). During these busy days when Filipinos visit cemeteries for the holidays, threat actors have seen a gateway to conduct Smishing attacks.

Several people reportedly received malicious SMS text messages impersonating local digital wallets. Based on the text messages received by random individuals, the Sender IDs used by the Smishing operators are the official Sender IDs used by the digital wallets for their SMS notifications.

Based on how the Smishing attacks are being delivered, security professionals, including Cyberint, are highly confident that these were conducted using IMSI-Catchers after correlating all the evidence and data from our sources.

BRAND

SOCIAL MEDIA IMPERSONATION



Cyberint observed a rising curve in terms of social media impersonations based on alerts raised to our Philippine clients.

Scam operators choose to build up fake social media profiles and conduct scam operations targeting gullible people by offering fake promotions and services. Fraudulent content associated with these fake profiles or pages is being distributed across different social media platforms through posting and advertisements (ads).



Samples of Social Media Fake Pages for Fraudulent Promotions



DATA EXPOSURE

DATA LEAKS

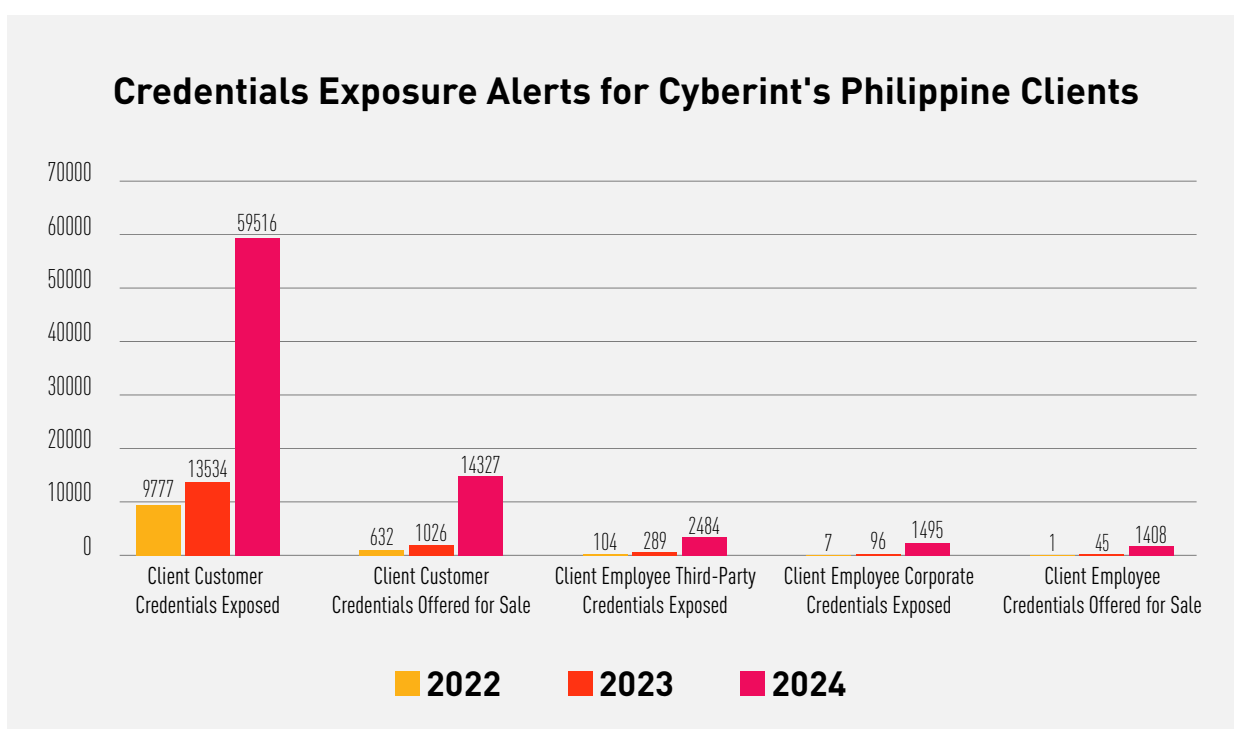
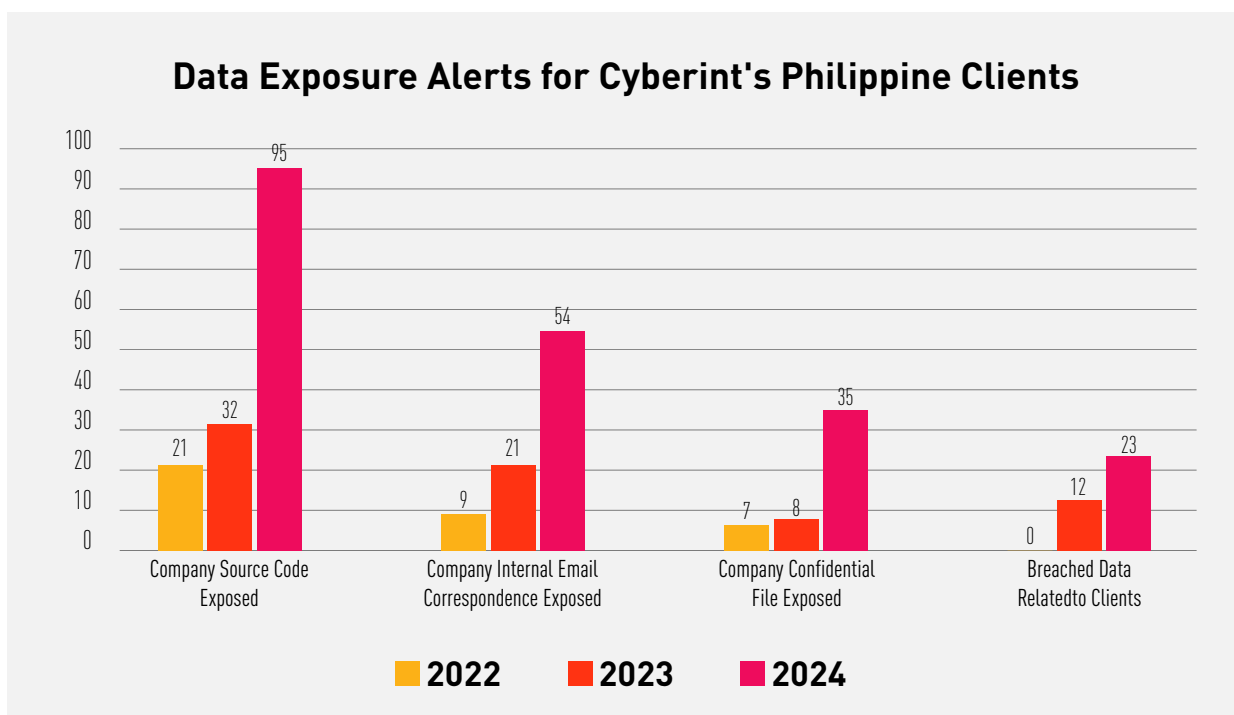
One of the significant highlights of 2024 is data leak incidents. Several data breach incidents have occurred in the Philippines, and they have been claimed by various local and global threat actors and groups, targeting several sectors, such as government, financial, retail, healthcare, education, and media.

DATA EXPOSURE

A rising curve in terms of data exposure for Cyberint, now a Check Point Company's clients has been observed over the past few years.

With the increase in Company Source Code exposure—mainly related to APIs (i.e., UAT, tokens, secrets, and requests), internal projects, and more—chances for threat actors to abuse these source codes for fraudulent activities will also increase.

Other exposed data, such as internal email correspondence and confidential files, can be utilized by threat actors to effectively plan their next steps and targets.



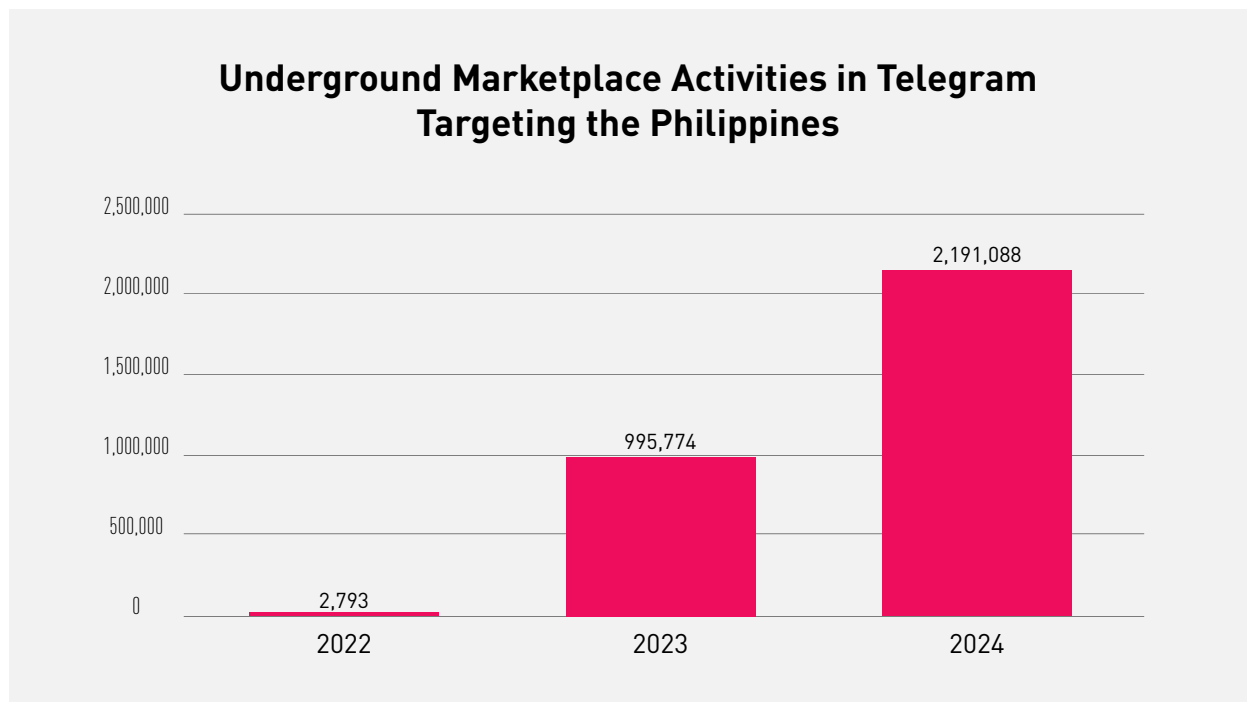
ATTACKWARE

As more technologies and services rise, threat actors ensure that they are catching up with these innovations. This has led to an increase in attackware being sold on the dark web.



UNDERGROUND MARKETPLACES

Cyberint, now a Check Point Company continuously monitors underground marketplaces, which offer several attackware and illicit services that can be used to conduct nefarious activities. In 2024, Cyberint observed a 100% increase in Telegram’s underground marketplace activities involving the Philippines compared to 2023.

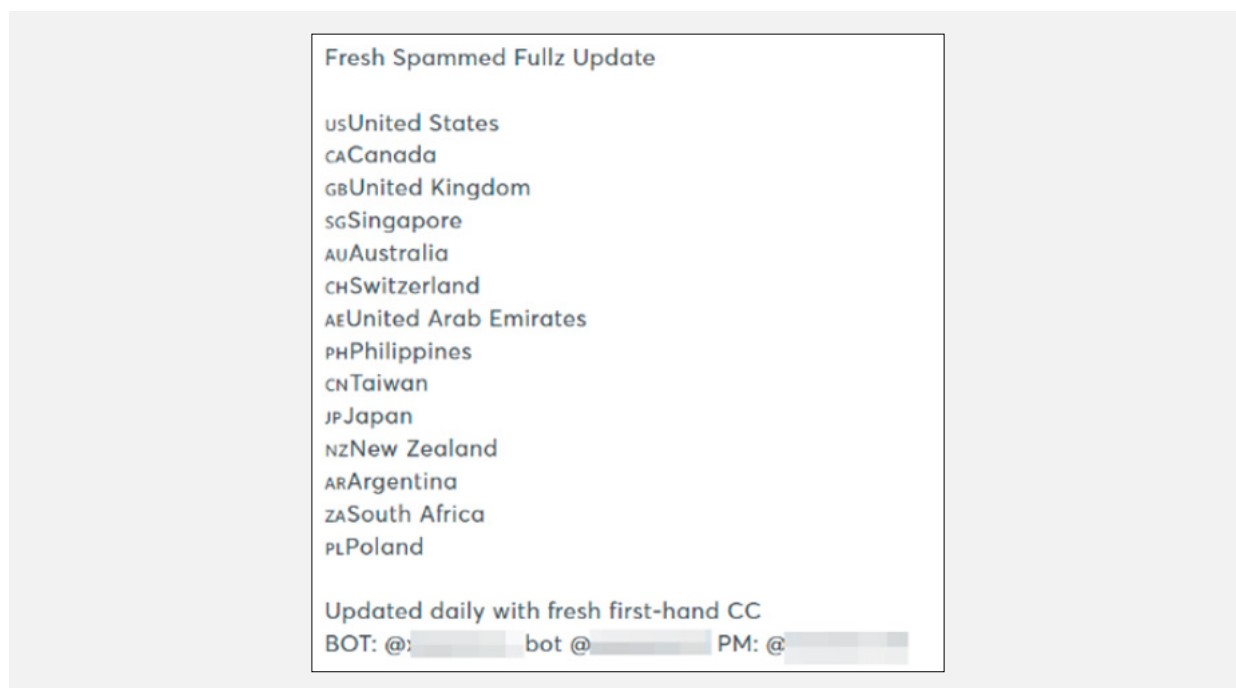


MALICIOUS TOOLS AND SERVICES

Some of the common items/services being offered in the underground are:

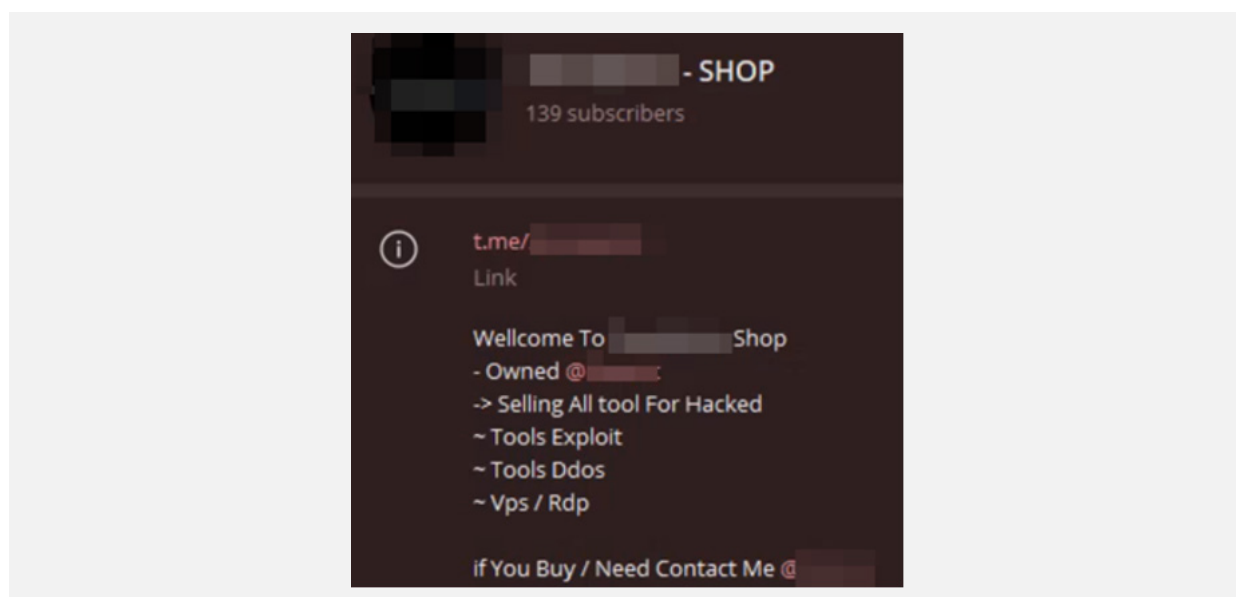
- **“FULLZ” – Full Information**

“FULLZ” is a slang term used by threat actors to refer to “Full information.” Mainly, this information is obtained by threat actors through several means, like Phishing, Carding, Malware, etc. This information is then traded in the underground, which other threat actors or scam operators can use to support their malicious campaign(s).



- **Exploit Tools and Attackware**

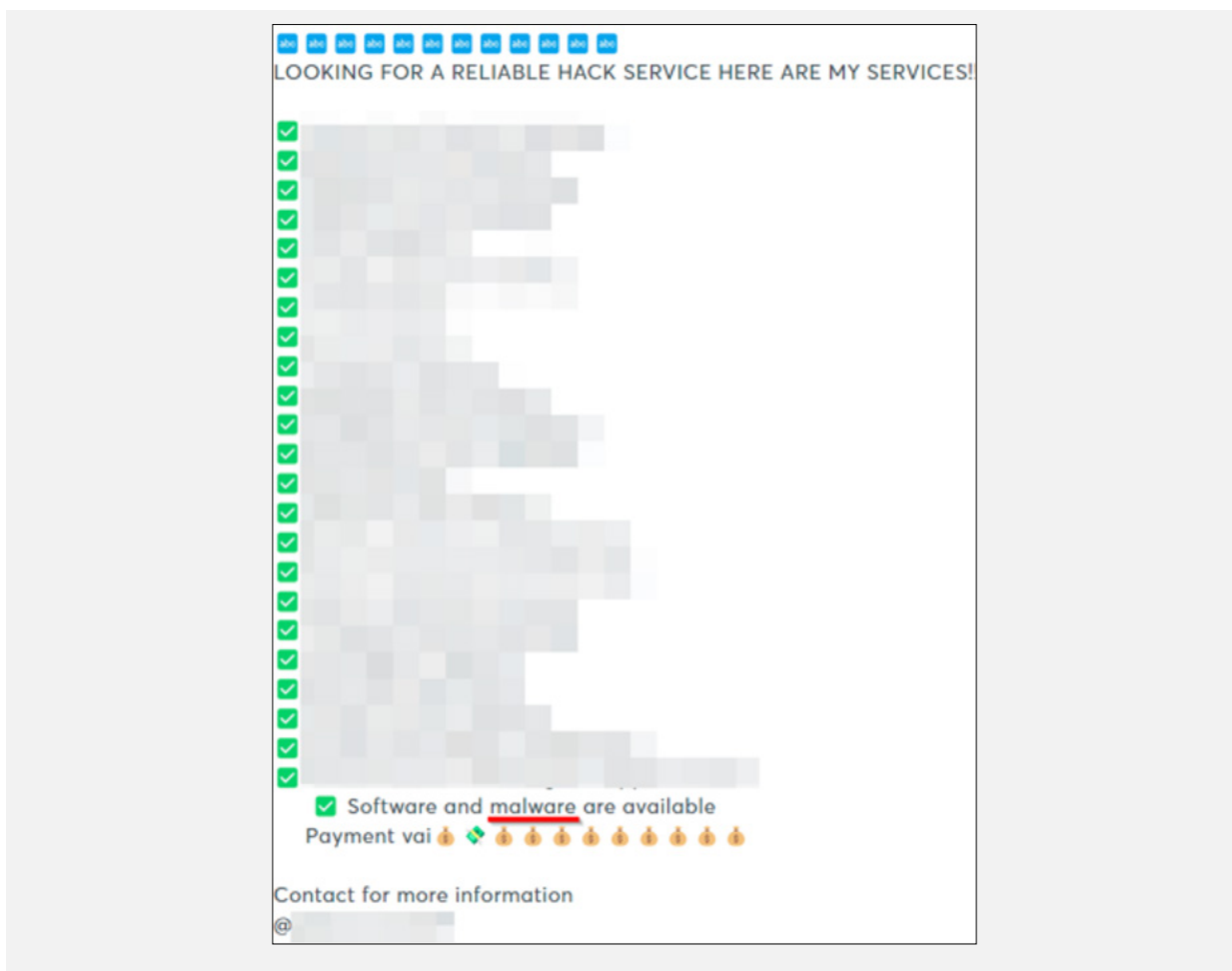
Some threat groups are selling or distributing attackware, such as Webshells, RDP, SSH Tools, and more.



Exploit Tools and Attackware Offered for Sale in the Underground

- **Malware / Malware-as-a-Service**

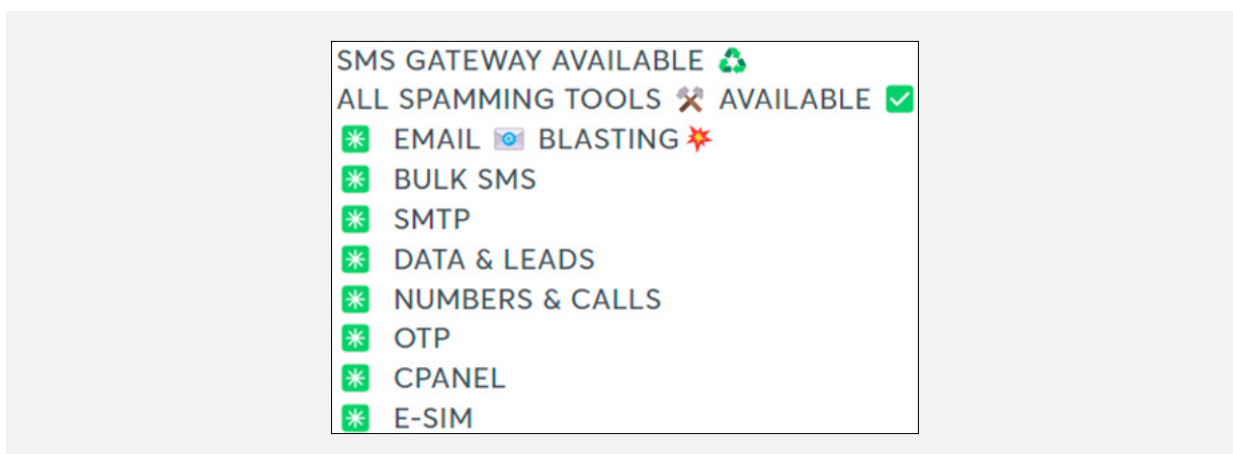
Other marketplaces are also offering malware, such as InfoStealer, Backdoors, and more.



Malware Samples and Services Offered in the Underground

- **Email and SMS Tools and Services**

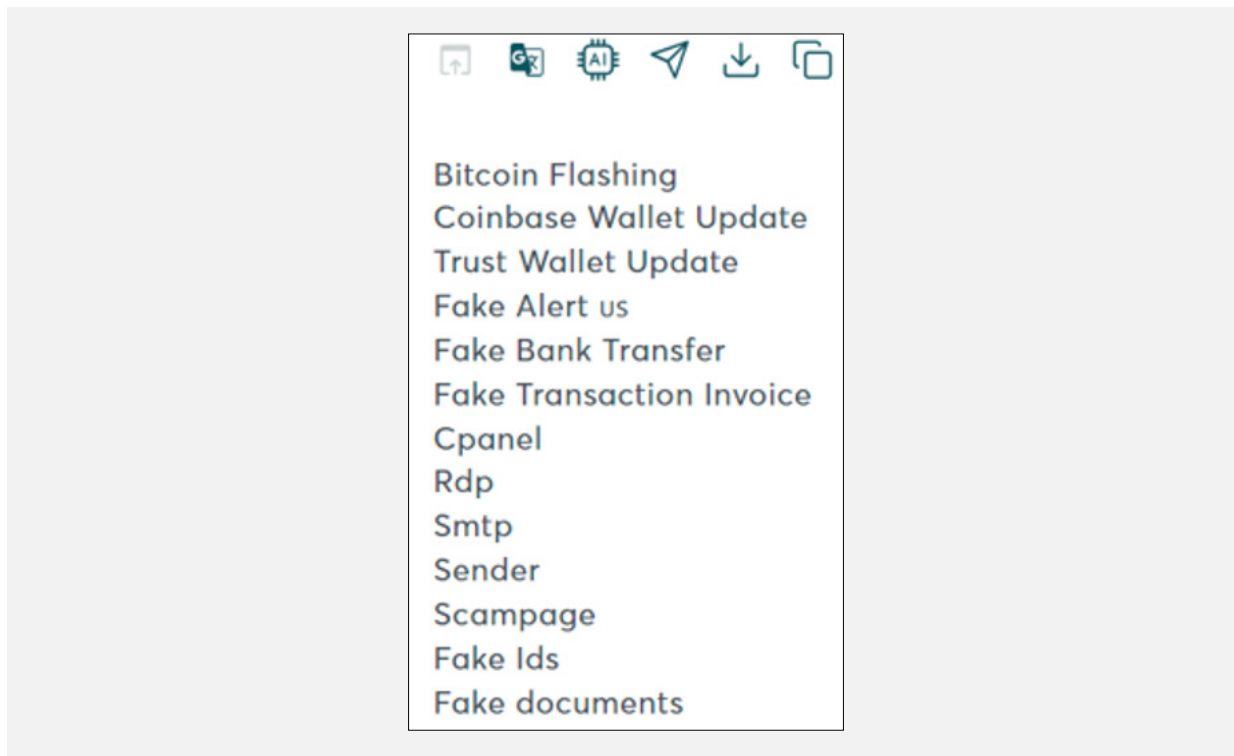
Many underground operators are offering SMS tools and services for spamming operations. For services, they mainly offer Bulk SMS, Email Blasting, cPanel, and many more. Meanwhile, for the tools, they usually offer SMTP, Phone Numbers, OTPs, e-SIM, etc.



Email and SMS Tools Offered for Sale in the Underground

- **Fake Documents**

Some underground operators are also selling fake documents that threat actors can use in their campaigns, mainly for social engineering activities like bypassing the Know-Your-Customer (KYC) process or Phishing. Samples of fake documents being sold in the underground include bank logs (statements, transactions, etc.), invoices, IDs, and more.

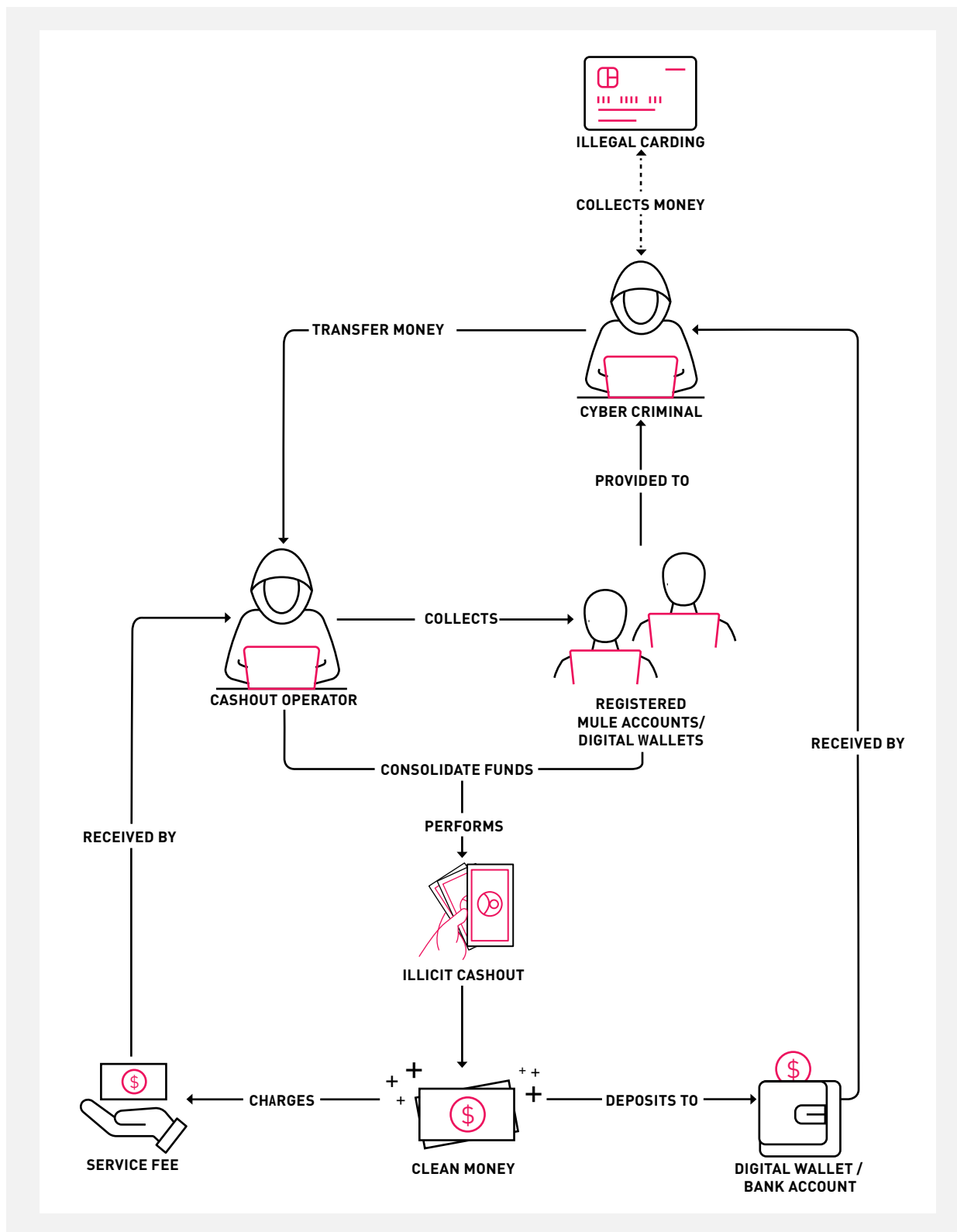


Fake Documents Offered for Sale in the Underground



- **Money Laundering – Fraudulent Cashout or Money Transfer Services**

Aside from technical tools and services offered in the underground, many offer post-operation schemes like money laundering through fraudulent cashouts or money transfer services using mule bank accounts, remittance accounts, or digital wallets.



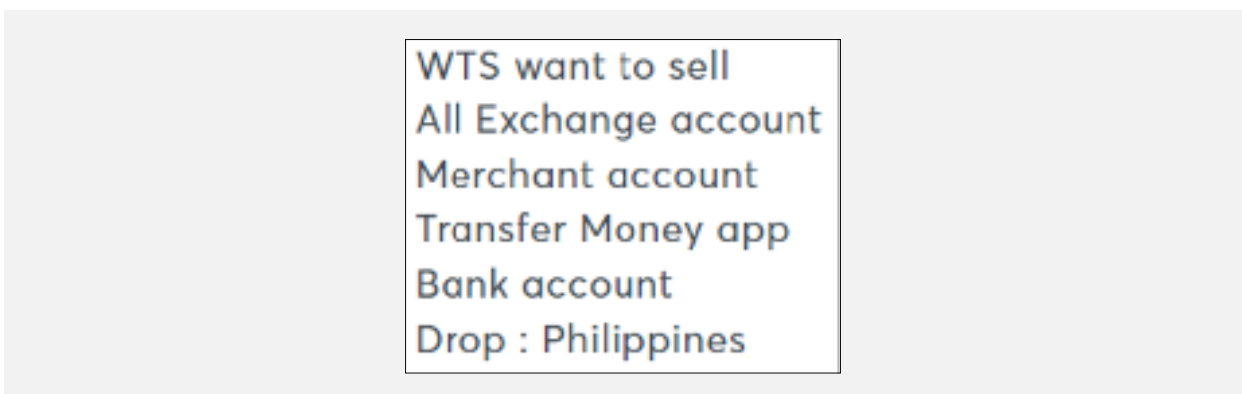
Money Laundering through Illicit Cashout Services – Flow Diagram



- **Mule Accounts**

In connection with the Money Laundering services offered in the underground, operators need mule accounts for fraudulent transactions. Therefore, many offer mule accounts for banks, digital wallets, and remittance services. These mule accounts are obtained either through carding activities, phishing, malware logs, or via **Quid Pro Quo**.

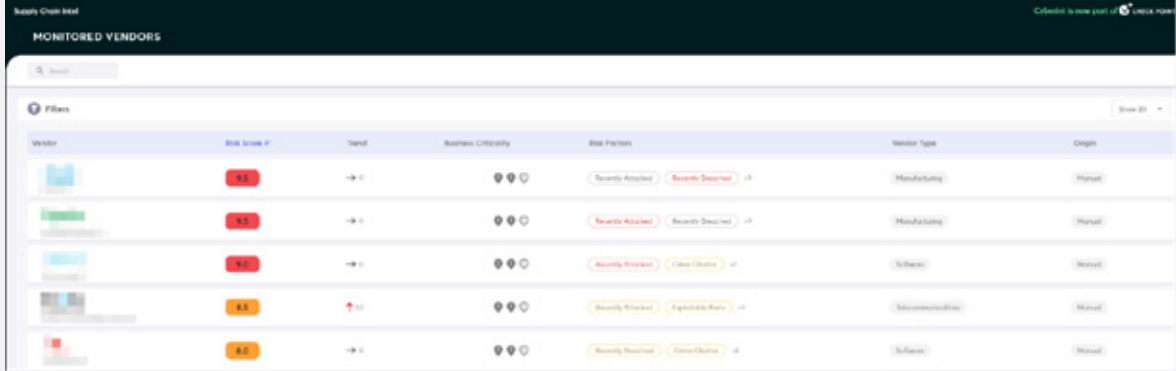
Quid Pro Quo—a Latin term for “**Something for Something**”—is a social engineering technique used by threat actors to obtain something (such as legitimate accounts) from an individual through bribery. For example, an illicit cashout service provider will look for individuals who are willing to sell their bank or digital wallet account in exchange for money without knowing how the buyer will use their account.



Selling of Mule Accounts in the Underground

SUPPLY CHAIN

With Cyberint, now a Check Point Company's latest technology, Supply Chain Intelligence, we were able to raise eight (8) Third-Party Vendor Breach alerts to our Philippine clients in 2024 within a few months, thus automatically notifying them based on the risk criticality and breaches circulating from our sources relating to any of their vendors configured within their Cyberint environments.



The screenshot displays the 'MONITORED VENDORS' interface. It features a search bar and a 'Filters' section. The main table lists vendors with columns for Vendor, Risk Score, Trend, Business Criticality, Risk Factors, Vendor Type, and Origin. The Risk Score column uses color-coded indicators (red for high, yellow for medium, green for low). The Risk Factors column includes labels like 'Security Breach' and 'Data Breach' with expandable arrows.

Vendor	Risk Score	Trend	Business Criticality	Risk Factors	Vendor Type	Origin
[Vendor Icon]	8.5	→	🔴🔴🔴	Security Breach Security Breach	Manufacturing	Manual
[Vendor Icon]	8.2	→	🔴🔴🔴	Security Breach Security Breach	Manufacturing	Manual
[Vendor Icon]	7.0	→	🔴🔴🔴	Security Breach Data Breach	Software	Manual
[Vendor Icon]	4.5	↑	🔴🔴🔴	Security Breach Exploitable Flaw	Manufacturing	Manual
[Vendor Icon]	8.0	→	🔴🔴🔴	Security Breach Data Breach	Software	Manual

Supply Chain Intelligence Module of Cyberint's



STAYING AHEAD OF THE CURVE: EVOLVING CYBER THREATS AND STRATEGIC PRIORITIES IN 2025

DEVICE AND GEO FILTERING MECHANISMS

As we approach 2025, the cyber threat landscape is set to become more intricate due to rapid technological advancements, changes in work environments, and geopolitical tensions (i.e., tensions between the Philippines and China regarding the South China Sea). The following key threats are anticipated to dominate the cyber security space in 2025, necessitating proactive planning and strategic responses from organizations across various industries.

Sophisticated Social Engineering and Phishing through Artificial Intelligence and IMSI-Catchers

Phishing attacks have long been a favored method for cyber criminals, but with the advent of Artificial Intelligence (AI), these attacks are set to become much more advanced. Threat actors will leverage AI to craft highly personalized phishing emails, texts, or social media messages tailored to individual targets by analyzing publicly available data. These AI-driven phishing campaigns will be challenging to detect due to their human-like language, dynamic content creation, and ability to evade traditional filters.

Aside from AI, threat actors will highly likely enhance their phishing operations by continuing the use of IMSI-Catchers to distribute smishing messages with spoofed Sender IDs, bypassing any validations from official telecommunication towers locally.

The rise in phishing attacks underscores the importance of robust security practices and the rapid adoption of advanced technologies to protect against these evolving threats.

With this advancement in social engineering methodologies, organizations will need to implement advanced AI-based defense mechanisms capable of identifying subtle anomalies in communication patterns to counter this growing threat. Additionally, security awareness training must evolve to help employees recognize these highly convincing phishing attempts.

Enhanced Brand Impersonation Techniques

In line with social engineering techniques, one of the easiest ways to conduct scam operations and fraudulent activities in the Philippines is through Brand Impersonation (a.k.a. Social Media Impersonation). Local scam operators will continue to create fake social media pages, impersonating a well-known brand, entity, or even high-ranking officials. Therefore, organizations should be equipped with brand and VIP monitoring tools to immediately detect fake social media pages or profiles before scam operators begin their operations.

Threat actors will start to leverage AI more, such as Deepfakes, for impersonation attacks, which was already observed in 2024. Deepfakes will highly likely be used to impersonate well-known people in the country and use these for fake advertisements on social media platforms.



Supply Chain Vulnerabilities

Supply chain attacks, where cyber criminals exploit vulnerabilities in third-party vendors or software suppliers, are expected to increase in 2025. As organizations depend more on external vendors for critical operations, this interconnectedness creates a larger attack surface for cyber threats. These attacks can disrupt entire supply chains by exploiting weaknesses in software update mechanisms or third-party cloud infrastructure. Attackers are likely to use these vulnerabilities to gain lateral access to corporate networks, steal sensitive data, or distribute malware. To mitigate these risks, continuous vendor security assessments, stricter contractual cyber security standards, and real-time monitoring of supply chain activities will be crucial.

Cyber Warfare Driven by Geopolitical Tensions

As the tensions between the Philippines and China regarding the South China Sea rise, threat actors in the Philippines initiated a campaign known as #OpChina. This campaign will mainly target Chinese-related entities and organizations as part of the local threat actors' ideology against the rising tensions between both countries. Meanwhile, over the past few months, some Chinese APT groups attempted to bribe some Philippine threat groups to conduct a cooperative attack against the Philippine government, whereas the local threat actors declined these offers.

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomom Kotohira Tower 25F,
1-2-8, Toranomom Minato-ku, Tokyo 105-0001

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: <https://cyberint.com> / checkpoint.com/erm

© Cyberint, 2024. All Rights Reserved.