FUTUREMATTERS™
CENTRE OF EXCELLENCE

JAPAN **CYBER THREAT** LANDSCAPE

March 2024

CONTRIBUTOR
Sharat Sinha
President, Asia-Pacific & Japan
Check Point Software Technologies Ltd

JAPAN
FINTECH
FESTIVAL™

INTRODUCTION

Threat Intelligence Overview

This document intends to provide a summary of the cybersecurity threats in Japan with reference to globally observed cyber landscape. It looks at various kinds of cyberattacks their quantum and impact as well as specific verticals that are targeted by various threat actors.

As in February, 2024, in Japan, an organization faces an average of 1003 attacks per week, with FakeUpdates being the top malware. Most malicious files are delivered via email, and Remote Code Execution is the most common vulnerability exploit. In recent times, major Japanese incidents include a sophisticated malware by a nation state, attacks on Nissan and JAXA, and data breaches at the University of Tokyo and CASIO. Globally, incidents include Ukrainian media hacks, a ransomware attack on U.S. schools, and disruptions in U.S. healthcare due to cyber-attacks. The document also covers trends in malware types, attack vectors, and impacted industries over the last 6 months.

The details provide an overview of the threat landscape and major incidents in Japan and globally, highlighting the prevalence of attacks, common malware types, and impact on various industries and organizations. The information described should create awareness and help businesses and government organization prepare well to safely operate in a digital environment.

Weekly impacted organizations by malware types:

	Ransomware	Mobile	InfoStealer	Banking	Botnet
Japan Avg.	1.40%	0.20%	1.30%	0.60%	2.00%
Global Avg.	2.60%	0.70%	2.50%	1.60%	3.30%

Threat Landscape

Ransomware Data Extortion – The ransomware operations pose significant challenges for the cyber criminals, therefore many groups chose to focus on data extortion instead of encryption. Many different types of information are considered sensitive, from corporate financial and proprietary data to personal data relating to health, financial data or any other personal identifiable information (PII), which makes the threat of data exposure even more potent.

Unrestrained Wipers - During 2022, there has been a noticeable shift in the scale of destructive malware deployment. Cyberespionage activity has been supplemented by destructive cyber operations, instigated by nations whose goal appears to be to inflict as much damage as possible.

Hacktivism - The boundaries between state cyber-operations and hacktivism have been blurred, as more hacktivist groups are now state – affiliated and promote nation state narratives . The hacktivist groups are better organized and more effective than ever before.

Cloud: Third Party Threat - There has been a significant increase in the number of attacks on cloud-based networks per organization, which shot up by 48% in 2022 compared with 2021 indicating a shift for threat actors' preference to scan the IP range of cloud providers gaining easier access to sensitive information or critical services.

Weaponization of Legitimate Tools - To combat sophisticated cybersecurity solutions, threat actors are developing and perfecting their attack techniques, which increasingly rely less on the use of custom malware and shift instead to utilizing non-signature tools.

For more data and examples please see Check Point Research Cyber Security: 2023 Annual Report.

Major Attacks And Data Breaches – Japan

- **Jan-24** - Researchers reported on a new and sophisticated malware used by China affiliated APT group, dubbed Blackwood. The malware was distributed via update mechanisms of legitimate popular software such as Tencent QQ, WPS Office, and Sogou Pinyin. The targets included Chinese and Japanese companies, as well as individuals located in China, Japan, and the United Kingdom.
- **Dec-23** - Japanese car manufacturer Nissan has confirmed a cyber-attack that affected Nissan Oceania, its Australian and New Zealand regional division, and took systems offline as a precaution. The company did not share specific information on the type or extent of the breach.

> **“Japan's space agency, JAXA, has disclosed that it had been hit by a cyber-attack”**

DATA BREACHES - GLOBAL

- **Dec-2**3 - Japan's space agency, JAXA, has disclosed that it had been hit by a cyber-attack. JAXA claimed that important rocket or satellite related operations information had not been affected, but that the breach is still being investigate. According to Japanese media, the attack had occurred in the summer, and was discovered by Japan's police a few months later.
- **Oct-23** - The University of Tokyo has experienced a data breach that impacted the personal information of students from the academic years of 2003 to 2022. The exposed data consists of more than 4K files containing addresses and grades, which were leaked as a result of malware infection that was distributed from a faculty members email.
- **Oct-23** - Japanese electronics firm CASIO has posted notice that more than 120,000 records of its customers from 149 countries was leaked, after hackers gained access to the company's ClassPad education platform.

> **“The cyber attack has disrupted healthcare services in pharmacies throughout the United States ”**

- **Oct-23** - American and Japanese security agencies have published a joint report detailing the activity of Chinese threat actor group BlackTech. The group has attacking entities in the United States and in Japan by targeting Cisco routers to gain initial access and maintain persistence in the target environments.

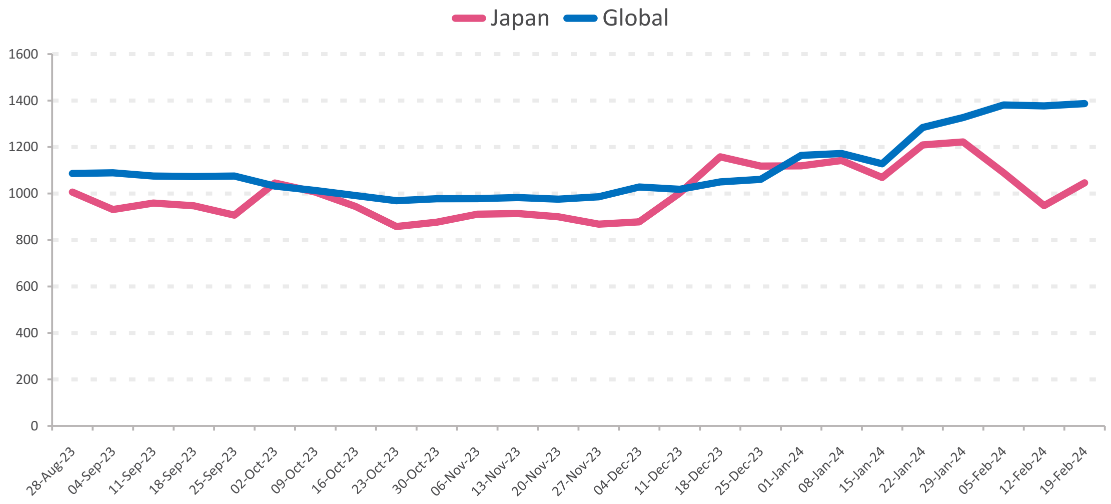
Major Attacks And Data Breaches- Global- Last Month

- Popular Ukrainian media outlets, including Ukrainska Pravda, one of the largest Ukrainian online newspapers, were hacked to spread the same piece of fake news of Russia destroying a unit of Ukrainian special forces. Ukraines state cybersecurity agency (SSSCIP) attributed the attack to a Russian threat actor but didnt specify which group was behind the incident.

DATA BREACHES - GLOBAL

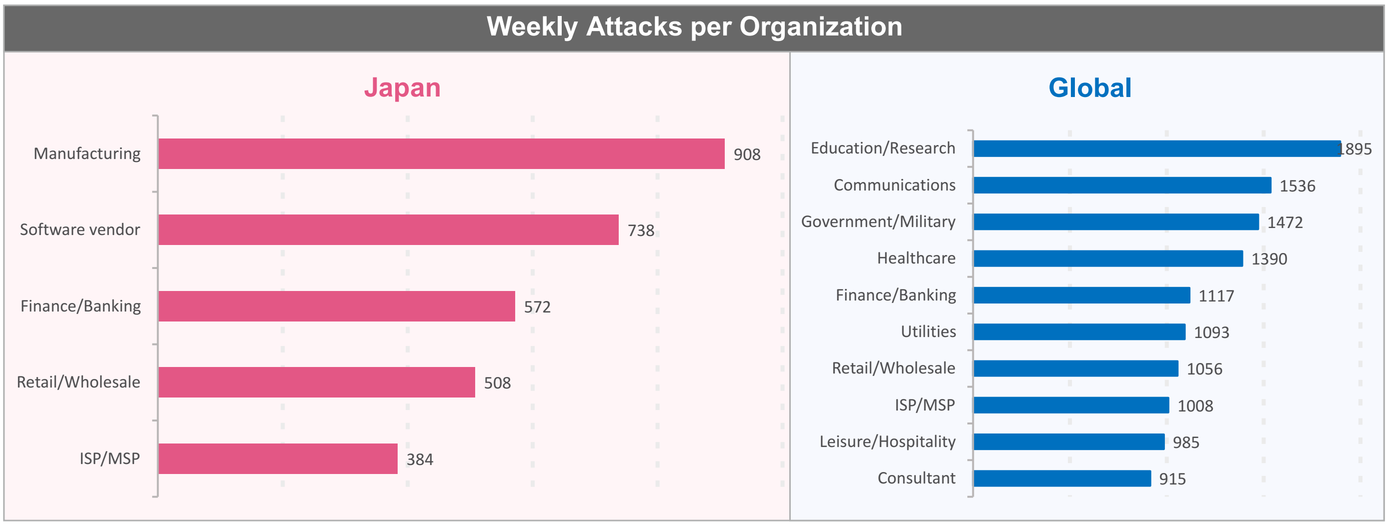
- The American Prince George's County Public Schools (PGCPS) has experienced a ransomware attack that compromised the personal data of nearly 100K individuals. The attack exposed individuals full names, financial account information, and Social Security Numbers. The Rhysida ransomware gang is reportedly responsible for the attack.
- The American health insurance giant United Health Group (UHG) has confirmed that its subsidiary OptumChange Solutions, which operates Change Healthcare platform, has suffered a cyber-attack which forced it to shut down systems. The attack has disrupted healthcare services in pharmacies throughout the United States. The firm claims that a suspected nation-state threat actor is behind the attack.
- The German control systems provider PSI Software SE has been a victim of a ransomware attack forced it to shut down external connections, and several IT systems including email systems, to prevent data exfiltration. No customer data has been compromised.
- The Israeli airline El Al has suffered a cyber-attack that affected the communication network of a plane flying from Thailand to Israel. The attackers have attempted to conduct a takeover over an area where the Iran-backed Houthis are active, however the plane reached its destination safely.
- Threat actor IntelBroker has claimed responsibility for a data breach on Los Angeles International Airport (LAX). IntelBroker leaked an alleged database consists of 2.5M records of confidential user data belonging to private plane owners, extracted from the airport's network. The database includes full names, CPA numbers, email addresses, company names, plane model numbers and tail numbers.

Attacks per Organization - Last 6 Months



TRENDS ACROSS INDUSTRIES

Most Impacted Industries - Last 6 Months



Top Malware - Japan - Jan-24

MALWARE FAMILY	JAPAN IMPACT	GLOBAL IMPACT	DESCRIPTION
FakeUpdates	2.0%	4.2%	Fakeupdates (AKA SocGholish) is a downloader written in JavaScript. It writes the payloads to disk prior to launching them. Fakeupdates led to further system compromise via many additional malware, including GootLoader, Dridex, NetSupport, DoppelPaymer, and AZORult.
Formbook	1.5%	1.9%	FormBook is an Infostealer targeting the Windows OS and was first detected in 2016. It is marketed as Malware as a Service (MaaS) in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.
Snatch	1.3%	0.6%	Snatch is a ransomware as a service (RaaS) group and malware, operating in a double extortion model, both stealing and encrypting victim data for extortion purposes. Snatch has been operating since 2018.
AsyncRat	1.0%	1.4%	Asyncrat is a Trojan that targets the Windows platform. This malware sends out system information about the targeted system to a remote server. It receives commands from the server to download and execute plugins, kill processes, uninstall/update itself, and capture screenshots of the infected system.
WikiLoader	1.0%	0.5%	WikiLoader is a downloader previously reported targeting Italian victims.

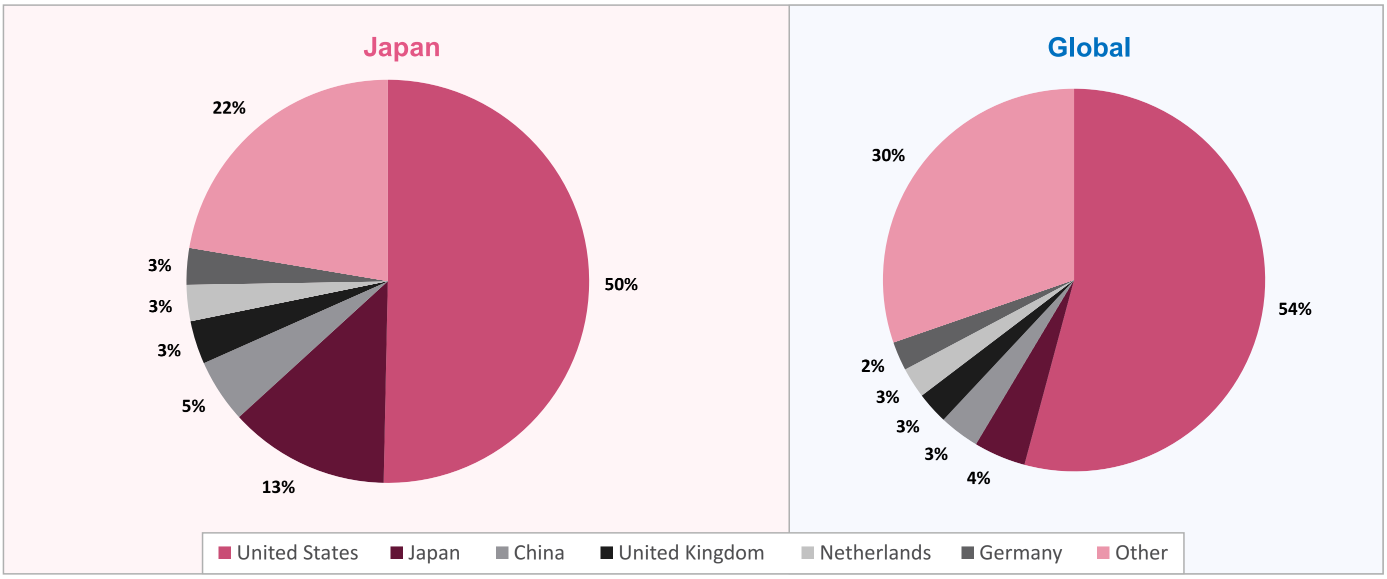
CYBER THREAT TRENDS

FUTUREMATTERS™ CENTRE OF EXCELLENCE

Top Malware - Global - Jan-24

MALWARE FAMILY	GLOBAL IMPACT	DESCRIPTION
FakeUpdates	4.2%	Fakeupdates (AKA SocGholish) is a downloader written in JavaScript. It writes the payloads to disk prior to launching them. Fakeupdates led to further system compromise via many additional malware, including GootLoader, Dridex, NetSupport, DoppelPaymer, and AZORult.
Qbot	3.3%	Qbot AKA Qakbot is a multipurpose malware that first appeared in 2008. It was designed to steal a users credentials, record keystrokes, steal cookies from browsers, spy on banking activities, and deploy additional malware. Often distributed via spam email, Qbot employs several anti-VM, anti-debugging, and anti-sandbox techniques to hinder analysis and evade detection. Commencing in 2022, it emerged as one of the most prevalent Trojans.
Formbook	1.9%	FormBook is an Infostealer targeting the Windows OS and was first detected in 2016. It is marketed as Malware as a Service (MaaS) in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.
Nanocore	1.5%	NanoCore is a Remote Access Trojan that targets Windows operating system users and was first observed in the wild in 2013. All versions of the RAT contain basic plugins and functionalities such as screen capture, crypto currency mining, remote control of the desktop and webcam session theft.
AsyncRat	1.4%	Asyncrat is a Trojan that targets the Windows platform. This malware sends out system information about the targeted system to a remote server. It receives commands from the server to download and execute plugins, kill processes, uninstall/update itself, and capture screenshots of the infected system.

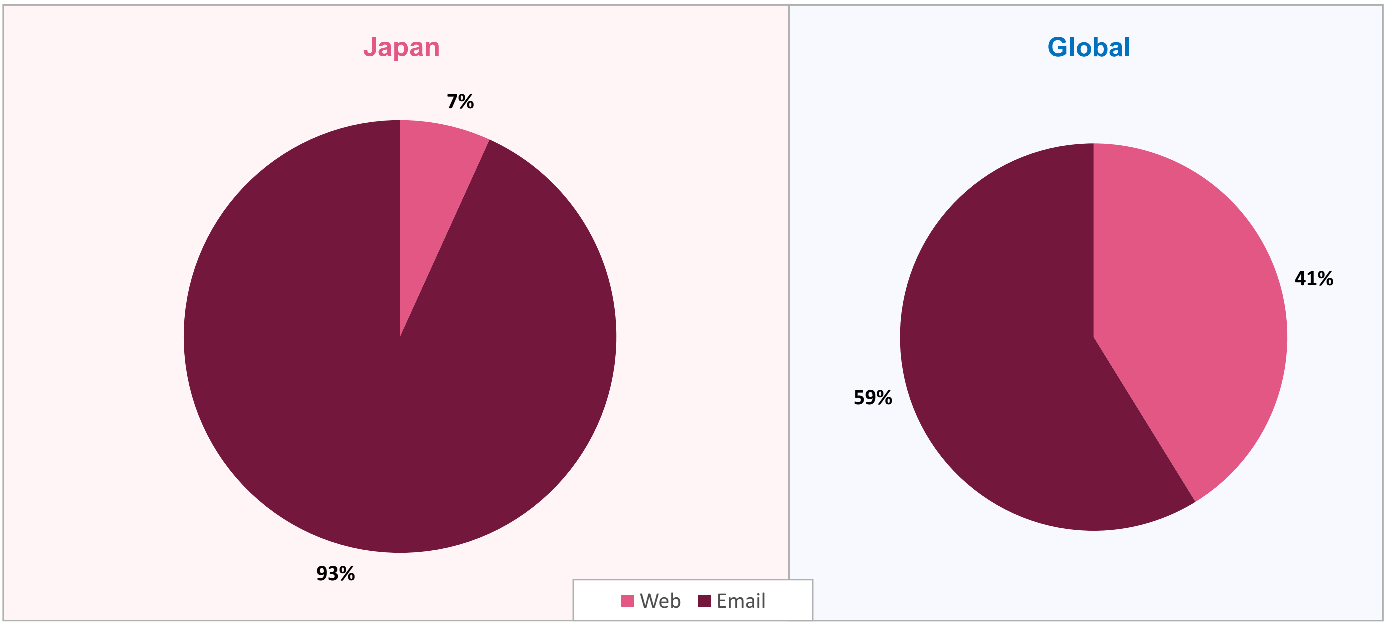
Top Threat Source Countries - Last 6 Months



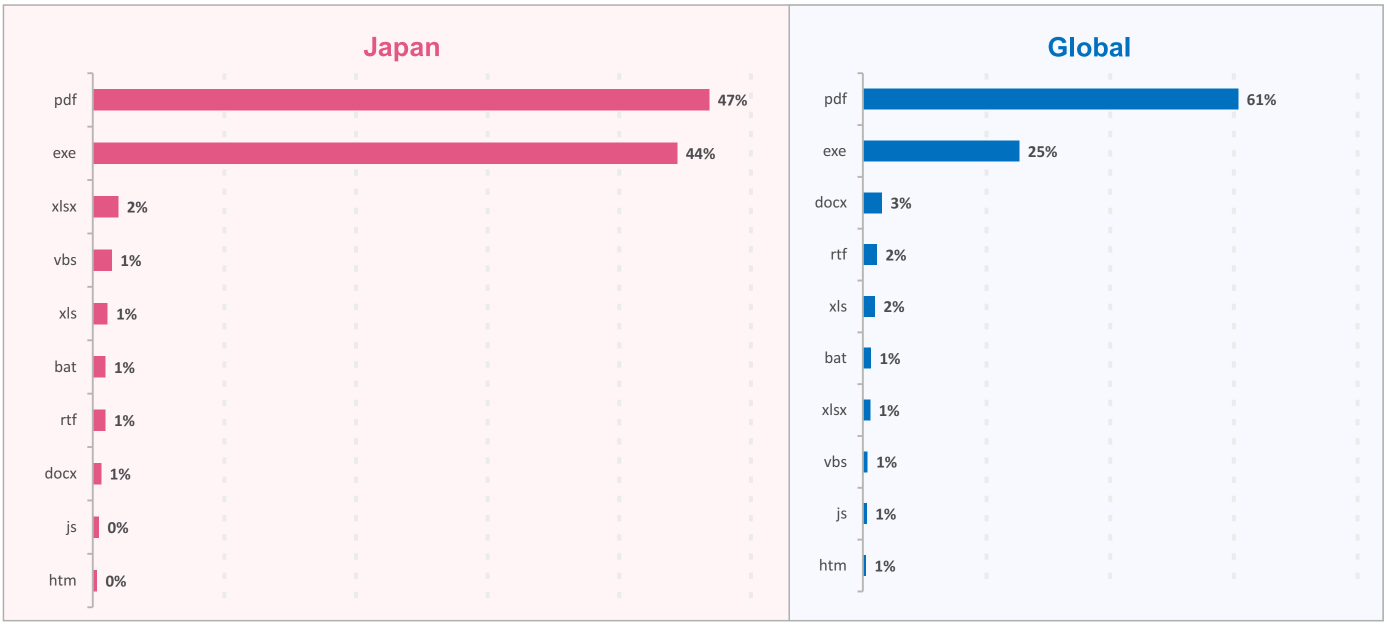
CYBER THREAT TRENDS

FUTUREMATTERS™
CENTRE OF EXCELLENCE

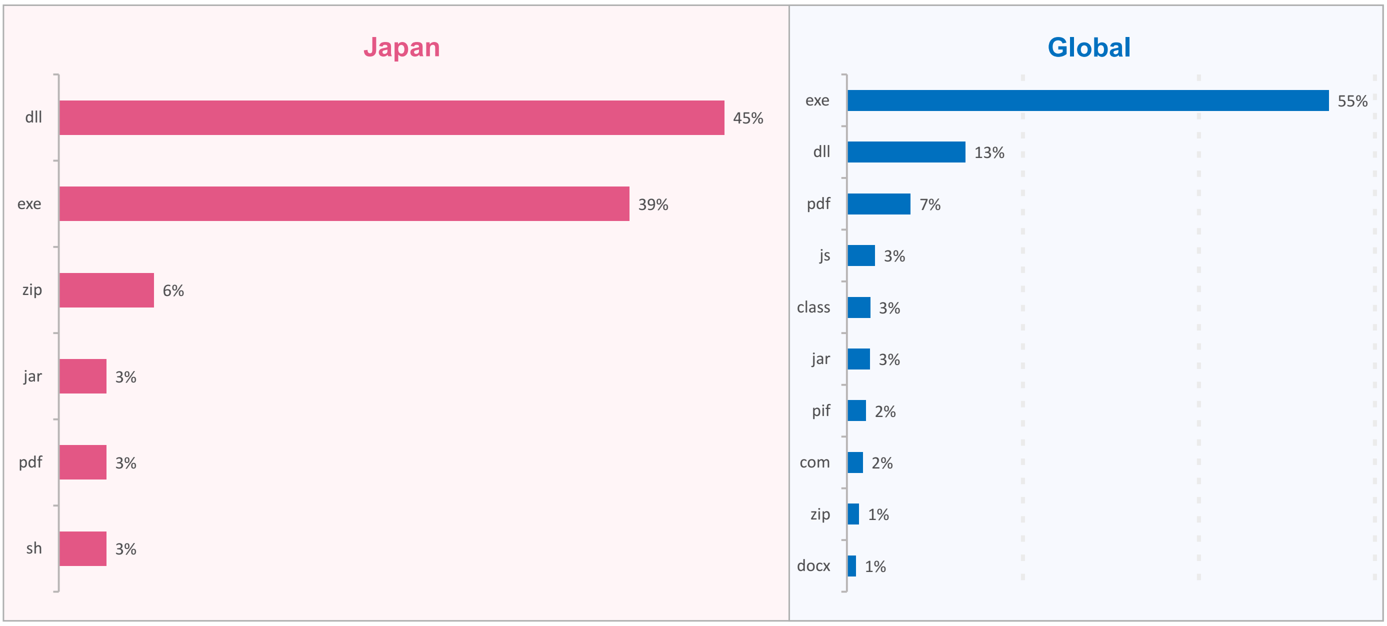
Attack Vectors for Malicious Files - Last 30 Days



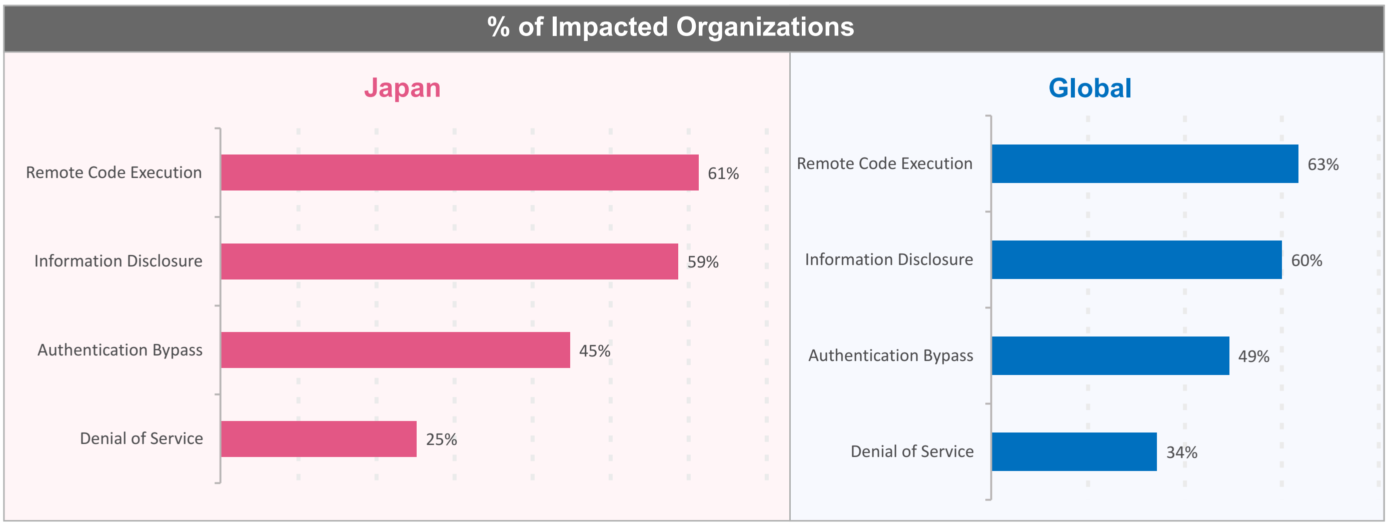
Top Malicious File Types, Email - Last 30 Days



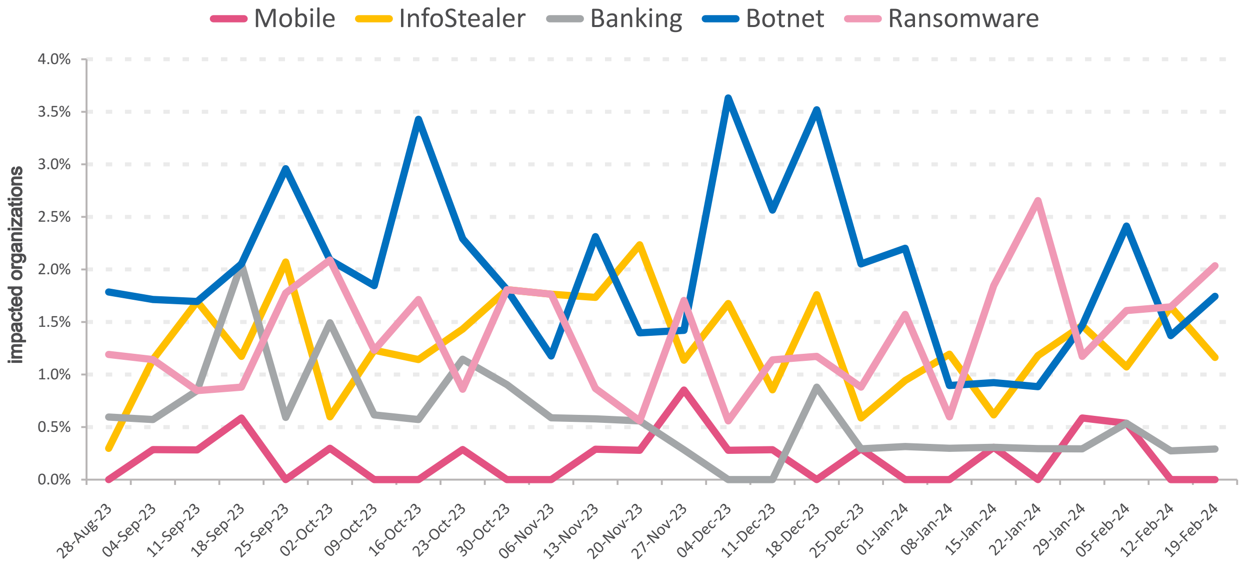
Top Malicious File Types, Web - Last 30 Days



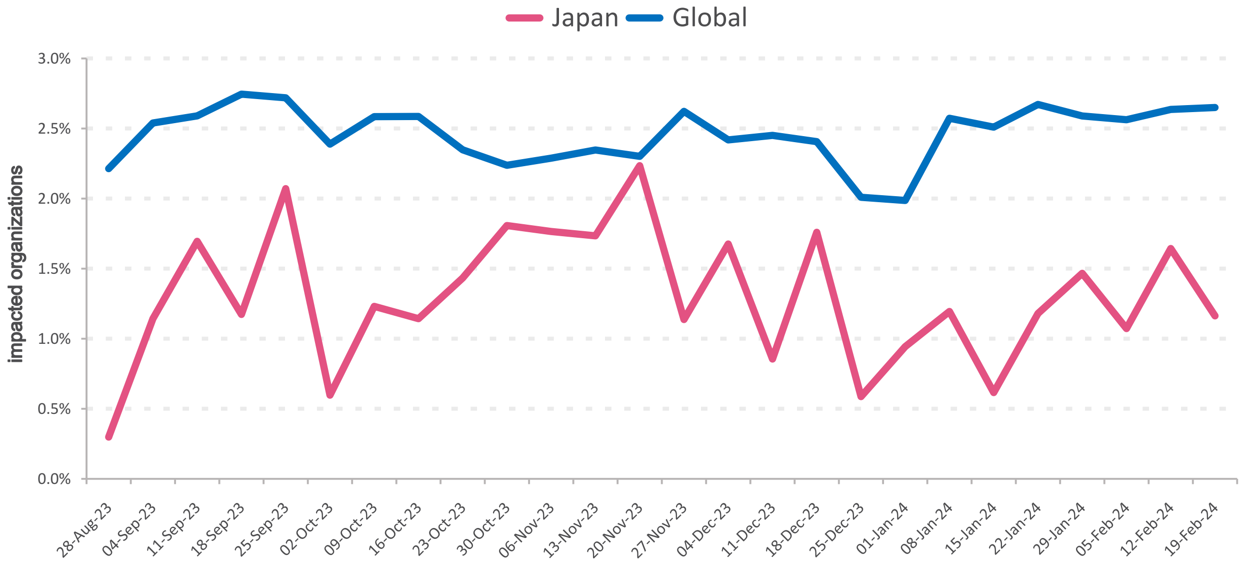
Top Vulnerability Exploit types - Last 30 Days



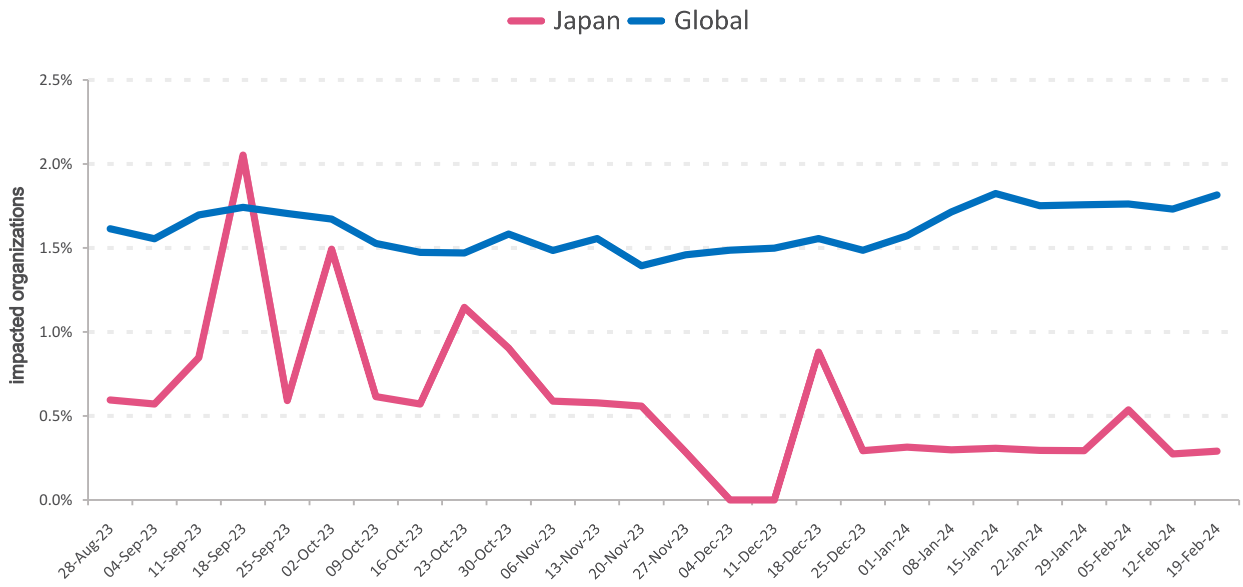
Major Malware Types Trend - Japan, Last 6 Months



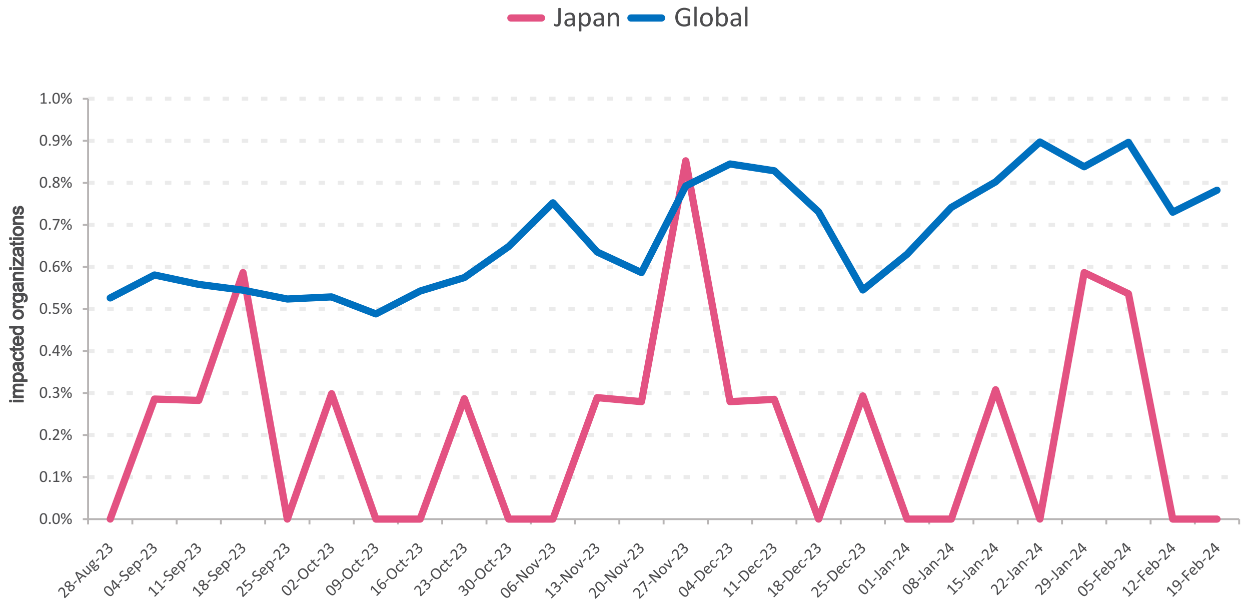
InfoStealer Attacks - Last 6 Months



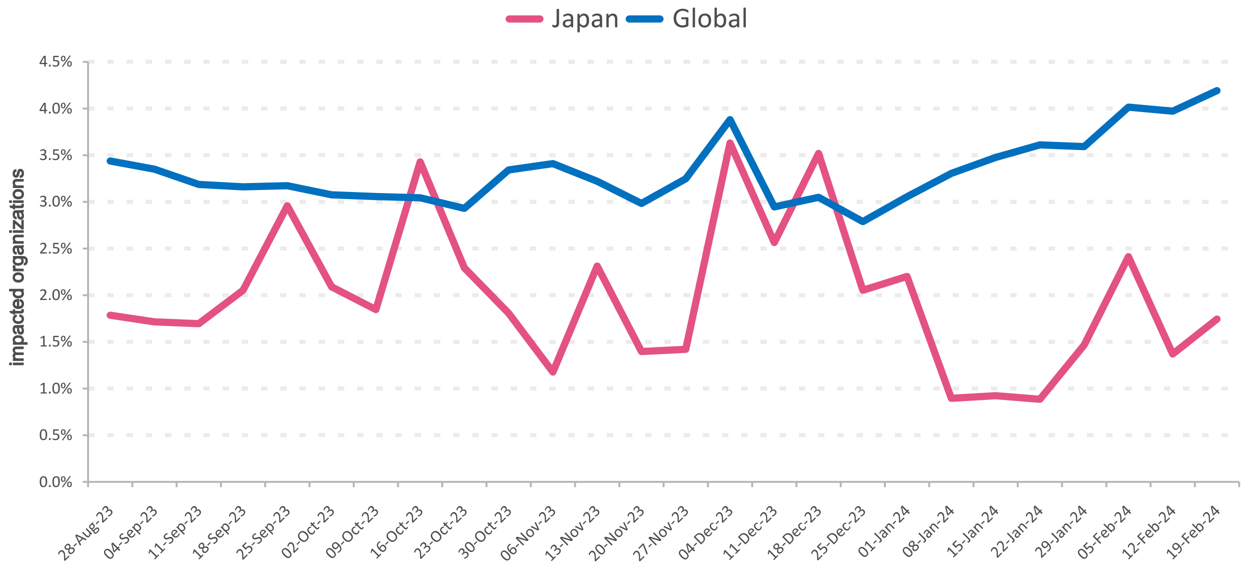
Banking Attacks - Last 6 Months



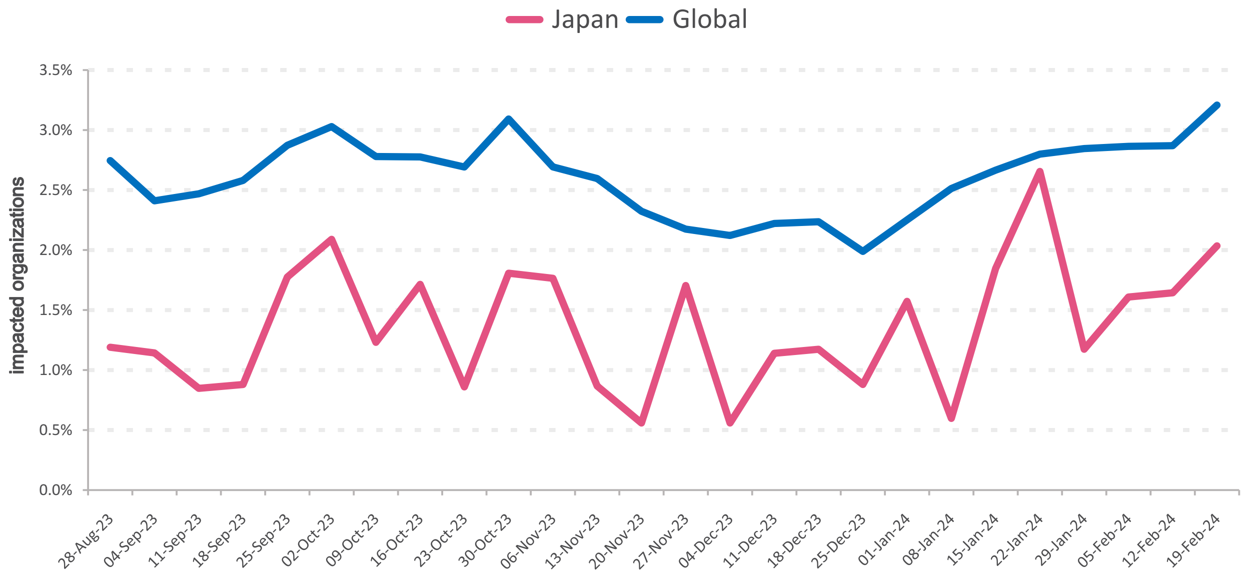
Mobile Attacks - Last 6 Months



Botnet Attacks - Last 6 Months



Ransomware Attacks - Last 6 Months



I write about Digital trust, Sustainable IT, Cyber resilience, Operational excellence, Strategic GTM and Organizational leadership.