ADARMA

TOGETHER WE'VE GOT THIS

THREAT LANDSCAPE REPORT

THREAT ACTORS, ATTACK TRENDS & RISKS TO CRITICAL NATIONAL INFRASTRUCTURE

Q1 2025

Contents

Purpose 03

Executive Summary 04

Adversaries & Malware Strains Tracked 05

Ransomware Trends 06

Critical National Infrastructure 09

Law Enforcement Actions Against Cybercrime 10

Q4 Threat Evolution 12

Recommendations to Mitigate Risks 15

How Adarma Can Help 16

Our Services 17

Purpose

The Adarma Threat Landscape Report provides a comprehensive overview of the key cyber threats that impacted the threat landscape during Q4 2024.

This report draws on intelligence compiled by Adarma's Threat Intelligence Team from both internal and external sources, with contributions from Adarma's partner Recorded Future.

The primary focus is on cyber activities between 1 October and 31 December 2024; however, information concerning cyber activity outside this date range will also be included if relevant.

We hope you find this report helpful. If you would like Hello@Adarma.com.

Executive Summary

In Q4, Adarma's Threat Intelligence Team tracked over 160 new or updated adversaries and malware strains.

- **Ransomware** remains a dominant force in the cyber threat landscape, with subgroups emerging from larger ransomware families.
- **RansomHub** remains the most active ransomware operation, reflecting a trend noted over the past three quarters of 2024.
- **Critical national infrastructure (CNI)** is still a prime target for nation-state-sponsored threat actors, ransomware groups, hacktivists and cybercriminals.
- **Nation-state-sponsored groups** from Russia, China, North Korea, and Iran have increased their activity.
- **Law enforcement operations**, such as Operation Endgame and Operation Cronos, disrupted prominent threat actors and infrastructure linked to hacktivism, ransomware, data breaches, social engineering, and Distributed Denial-of-Service (DDoS).
- **Data leak sites** have begun to lose credibility, with many of the leaks posted duplicating earlier attacks or inaccurately being linked to the LockBit ransomware group.
- **Threat actors** increasingly leveraged file hosting services to carry out business email compromise (BEC) attacks.
- **Scalable Vector Graphics (SVG)** attachments and ZIP file concatenation were observed being used to boost phishing campaigns and bypass detection systems.
- **Botnet infrastructure** was rebuilt to perform password-spraying attacks specifically targeting Microsoft customers.
- **Threat actors and advanced persistent threat (APT) groups** developed new ways to use ClickFix in social engineering campaigns, such as phishing and malvertising. In one observed campaign, this led to the deployment of info-stealing malware and loaders, specifically LummaStealer and Amadey.

Adversaries & Malware Strains Tracked

These images show the number of adversaries and malware strains the Adarma Threat Intelligence Team tracked during Q4 2024.

These statistics are based on intelligence gathered and information monitored in Adarma's Threat Intelligence Platform (TIP) throughout the quarter.

62
out of 386

New or Updated
Adversaries Tracked

98
out of 528

New or Updated
Malware Strains Tracked

This figure shows the number of adversaries and malware strains tracked by the Adarma Threat Intelligence Team in Q4 2024.

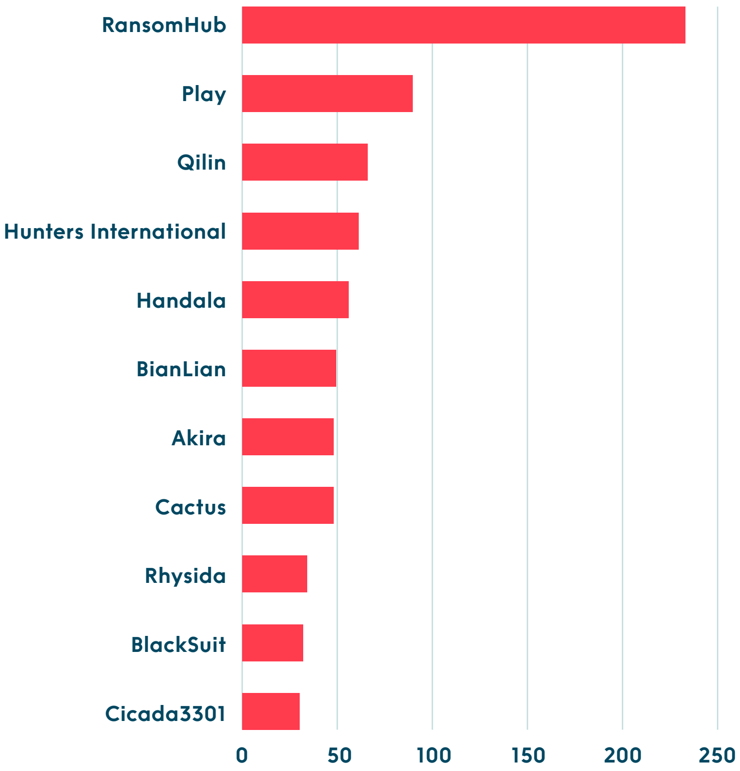
Ransomware Trends

Ransomware continues to thrive as one of the most profitable forms of cybercrime, with RansomHub, LockBit, and Play ranking as the top three most active threat actors, as shown in the figure shown here.

RansomHub

RansomHub stands out as the most prevalent group. Since its emergence in February 2024, this Ransomware-as-a-Service (RaaS) operation has targeted many industries and is widely viewed as the leading ransomware threat, a position previously held by LockBit in 2023. For more details on RansomHub's rise as a major RaaS provider, please see Adarma's RansomHub threat profile.

Ransomware:



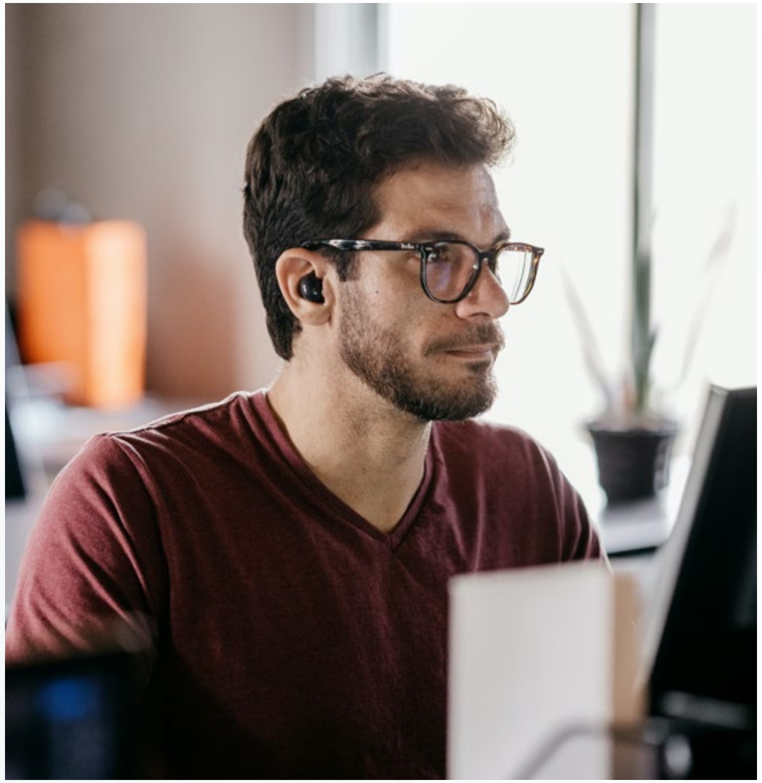
LockBit

In 2024, LockBit faced several law enforcement actions including Operation Cronos in February 2024, the indictment of its key operator Dmitry Yuryevich Khoroshev in May, and the arrest of Rostinav Panev, who was allegedly arrested in August 2024 for developing and maintaining LockBit's infrastructure. Despite these setbacks, the group has shown resilience in rebuilding its operations. However, a Trend Micro report suggests LockBit may be overstating its comeback, as many victims on its new data leak site appear to be re-uploads of old attacks or misattributed.

On 19 December 2024, LockBit announced plans to release LockBit 4.0 by February 2025, indicating ongoing activity and improvements to its RaaS offering. We expect LockBit's activity to continue rising in 2025. The group has also influenced emerging ransomware operators, such as SafePay and Helldown, which use a leaked LockBit encryptor. This highlights the value of LockBit's malware and tactics in cyber operations. Bashe, also known as APT73, and listed in Figure 1's top ten, have also reportedly adopted LockBit's operational techniques.

Play

Play favours high-value targets, often aligned to CNI sectors, including energy, utilities, transport and education. The group are known to exploit software vulnerabilities to gain access to systems and operate a RaaS affiliate model. In October 2024, reporting indicated that the group collaborated with threat actors affiliated with North Korea's Reconnaissance General Bureau during a ransomware attack conducted in September 2024.



Emerging Ransomware Groups

In Q4 2024, several new ransomware groups emerged, most notably KillSecurity, Bashe and Lynx. These groups demonstrated rapid growth and targeted industries worldwide, with their source code closely mirroring that of existing variants. This resemblance suggests they may be rebrands or offshoots of established ransomware operators.

KillSecurity

KillSecurity, originally a hacktivist group that first appeared in 2023, rose to become the fourth most active ransomware group this quarter. It has targeted sectors such as retail, transport, healthcare, and construction, commonly exploiting vulnerabilities and conducting phishing campaigns to gain initial access. In June 2024, the group launched a RaaS model, which may have contributed to a significant increase in attacks later in Q4.

Bashe

In Q4, Bashe actively targeted organisations in the healthcare, financial services, technology, and retail sectors. The group leverages various tools to maintain persistence and evade detection. As noted, it is reportedly linked to LockBit affiliates by adopting many of the same operational techniques.

Lynx

Active since July 2024, Lynx has targeted retail, real estate, construction, manufacturing, and financial services across the UK and US. According to recent reports, its ransomware encryptor closely resembles the INC Ransom source code, suggesting a potential link or that Lynx acquired it. In May, INC reportedly sold its source code on underground marketplaces and altered its infrastructure, raising the possibility that Lynx obtained the code prior to launching operations.

FOG

FOG first appeared in April 2024 and targeted a range of sectors in Q4, including manufacturing, healthcare, transport, telecommunications, energy, and utilities in North America, Europe, and Asia. A report by SentinelOne indicates that FOG heavily relies on exploiting known vulnerable applications and often purchases credentials from Initial Access Brokers (IAB) to gain entry.

Critical National Infrastructure

CNI organisations remain a prime target for nation-states, ransomware groups, hacktivists, and cybercriminals, driven by motives ranging from espionage and financial gain to the theft of sensitive data and disruption of critical services.

Below are notable attacks on CNI organisations in Q4:

OCTOBER

01

In the first half of October, a joint cybersecurity advisory was issued regarding the Russian Federation's Foreign Intelligence Service and its recent exploitation of vulnerabilities. This advisory was directed at both CNI and other organisations, warning them of a global campaign in which more than 20 known vulnerabilities were being exploited.

02

Following the advisory, additional reports signalled a rise in attackers exploiting vulnerabilities, including zero-day flaws. This trend highlights the need for effective vulnerability management that quickly identifies assets and implements security updates.

03

Around the same time, Microsoft and the US Department of Justice seized more than 100 domains and dismantled attack infrastructure linked to Russian-state sponsored group ColdRiver, also known as Callisto, Seaborgium, or Star Blizzard. ColdRiver have previously targeted CNI organisations including energy, government and defence through spearphishing campaigns.

04

In the middle of October, CISA released a joint cybersecurity advisory highlighting activity by Iranian threat groups, detailing their use of brute force and other techniques to gain access to CNI organisations. Once compromised, these Iranian actors were selling that access on dark web forums. Affected sectors included healthcare, government, information technology (IT), energy and engineering sectors.

05

Towards the end of October, OpenAI reported that CyberAv3ngers, a group linked to the Iranian Islamic Revolutionary Guard Corps, had used AI tools to support cyber-attacks against industrial control systems and programmable logic controllers. These systems are commonly found in sectors such as energy, water and manufacturing.
By applying AI in coding and vulnerability research, the group improved its reconnaissance and overall operational effectiveness.

Law Enforcement Actions Against Cybercrime

ADARMA
TOGETHER WE'VE GOT THIS

In Q4, law enforcement took decisive action against cybercrime, arresting individuals linked to some of 2024's most notorious cyber threats. These arrests involved hacktivism, data breaches, ransomware, social engineering campaigns, and DDoS activity.

Hacktivism

On 16 October, two Sudanese nationals were charged in the US for their involvement in operating the hacktivist group Anonymous Sudan. Believed to have been active since January 2023, this cybercriminal organisation collaborated with pro-Russian hacktivist groups such as KillNet and SiegedSec, launching DDoS attacks against entities linked to critical national infrastructure.

Victims included hospitals, technology firms, and government agencies worldwide. Anonymous Sudan developed and deployed its own DDoS tool, called Skynet-Godzilla, which it reportedly sold it to other criminal groups on underground marketplaces.

Data Breach

On 30 October, US officials detained Alexander Moucka in Canada. He is under suspicion for his alleged involvement in more than 165 data breaches, which resulted from his theft of login credentials belonging to users of SnowFlake's cloud services. Many accounts lacked multi-factor authentication (MFA), allowing access to credentials, some dating back to 2020. The breach affected sectors such as financial services, retail and education.

Ransomware

In early November, Evgenii Ptitsyn, a Russian national, was extradited from South Korea to the US and appeared in a Maryland federal court on 4 November. Ptitsyn faces 13 criminal charges for his implication in the Phobos RaaS operation. Over the years, the operation is believed to have extorted more than £12 million in ransomware payments and targeted over 1000 organisations globally, including attacks on emergency services, healthcare and other CNI entities.

Social Engineering

In late November, law enforcement charged five members of the group Scattered Spider for the targeting of companies worldwide using social engineering tactics designed to steal credentials and commit identity theft. Their activities allegedly involved stealing cryptocurrency, personal information and intellectual property worth millions. Court documents indicate that the members conducted phishing campaigns between September 2021 and April 2023. They sent SMS messages warning that victims' accounts would be deactivated, including links to fake login pages that mimicked legitimate websites. These messages often appeared to come from the victim's company, a contracted business information provider, or a supplier associated with the victim's organisation.

DDoS Attacks

Operation Power-Off is a joint law enforcement initiative targeting 27 popular DDoS platforms. At the time of this report, the operation has successfully resulted in the arrest of four individuals, the confiscation of 18 booters, the shutdown of 27 domains, and the identification of over 320 users involved in the illicit activities. The operation seeks to dismantle the infrastructure supporting these platforms while introducing measures to prevent future incidents.

Resurgence Following Law Enforcement

Q4 saw the resurgence of malware that had been disrupted earlier in the year, namely Bumblebee and Smokeloader malware. Operation Endgame had limited their spread in May, yet both have reappeared and are now distributed through phishing emails.

In the Bumblebee campaign, a phishing email instructed victims to download a compressed folder containing a .lkn file. This file used PowerShell to download a .msi file disguised as a legitimate installer, which then executed malware in memory. The attack chain mirrors earlier Bumblebee campaigns that used phishing and malvertising as initial infection vectors.

Since September, SmokeLoader has targeted Taiwan-based entities in healthcare, IT and manufacturing. First identified in 2011, SmokeLoader was mainly used to deliver secondary payloads. Recent incidents show the malware being used directly in attacks. These attacks began with phishing emails containing Excel attachments that exploited vulnerabilities CVE-2017-0199 and CVE-2017-11882. The malware, known for its data theft capabilities, has also been linked to Phobos and 8Base.

Q4 Threat Evolution

In Q4, the Adarma Threat Intelligence Team observed a marked evolution in threat tactics, as threat actors refined their methods to circumvent traditional security measures. This section examines emerging trends, ranging from advanced social engineering and phishing techniques to increasingly sophisticated botnet activity.

ClickFix

Social engineering remains a common tactic among threat actors, who trick users into disclosing credentials or installing malware. One method that has evolved over the past six months is ClickFix. Initially observed in phishing campaigns, it has now expanded into malvertising.

How it Works

ClickFix deceives victims by displaying a fake browser or application error message that prompts them to execute specific keyboard shortcuts. These actions trigger encoded PowerShell commands which download and install malware onto the system. In Q3, attackers embedded malicious HTML links in phishing emails. When recipients clicked these links, they were shown a message promising to “fix” an issue and instructed to paste and run a hidden command, compromising their systems.

ClickFix Activity

In Q4, threat actors and APTs began leveraging ClickFix in malvertising campaigns. In October, transport and logistics firms were targeted with info-stealing malware such as LummaStealer and Amadey. Attackers disguised fraudulent Google Meet pages to prompt users into running executing malicious PowerShell commands.

In response to the surge in LummaStealer and Amadey, Adarma analysed the malware and released Emerging Threat packs to managed SOC customers for proactive threat hunting. Other campaigns used fake reCAPTCHA pages that prompted victims to perform the same keyboard shortcuts to bypass a fabricated challenge. Threat actors exploited advertisement networks and traffic distribution systems to redirect users to these deceptive pages, ultimately resulting in malware infections.

A separate campaign, attributed with medium confidence to APT28 (a group linked to Russia’s Main Intelligence Directorate), was also observed. In October, Ukraine’s Computer Emergency Response Team issued an advisory detailing how the group used phishing emails to install Metasploit and secure shell tools and to harvest browser data from government entities.

BEC: Attacks Via File Hosting Services

File hosting platforms have become integral to business operations, providing seamless file storage and collaboration. Their widespread use, however, has attracted threat actors who exploit the trust organisations place in these services. Cybercriminals use these platforms to carry out financial fraud, exfiltrate sensitive data, and move laterally within networks.

Microsoft's recent Q4 report highlighted the increasing use of file hosting services in phishing emails to facilitate BEC attacks. Threat actors manipulate access controls by restricting shared files so that only the intended recipient can view them. This tactic not only bypasses standard security defences but also enhances the credibility of the email by prompting victims to sign in or re-authenticate. Victims are sometimes asked to sign in or re-authenticate, adding an extra layer of perceived legitimacy. Another tactic involves sharing files in view-only mode, which stops security teams from downloading the file for deeper analysis and makes detection more difficult.

Threat actors have also been observed misusing DocuSign's Envelopes API to impersonate brands like Norton and PayPal, sending convincing fake invoices at scale and prompting victims to sign documents authorising payments. By using legitimate DocuSign accounts, likely obtained via compromised credentials, attackers can bypass certain detection systems because the emails originate from the genuine DocuSign domain (docusign.net).

Phishing: Defence Evasion With .zip and .svg

In Q4, reports highlighted a novel phishing method used by threat actors to bypass detection and distribute malware. This technique exploits how certain archive tools process combined .zip files. By merging multiple .zip files, attackers hide malicious content, and in some cases, only benign files are displayed, allowing the malware to evade detection. However, .zip file concatenation was not the only method observed during Q4.

Attackers also used Scalable Vector Graphics (SVG) attachments to spread malware. Although the SVG format was designed for graphical text representations, it can embed HTML phishing forms and JavaScript code. Threat actors leveraged these features to steal credentials or redirect victims to phishing sites disguised as legitimate content.

In addition, corrupted Word documents were deployed as email attachments in an effort to evade detection. Although they appeared corrupted to some systems, the documents remained easily recoverable within the application. Many contained QR codes that led recipients to phoney Microsoft login pages designed to harvest their credentials.

Botnet Activity

In Q4, various botnet activities were observed, including APT groups targeting Microsoft customers with password-spraying attacks and efforts to rebuild botnet infrastructure following law enforcement disruptions.

Quad7 Botnet and Storm-0940

In late October, Microsoft reported password-spraying attacks against multiple customers that resulted in stolen credentials. These attacks were linked to the Quad7 botnet, also known as 7777, which primarily comprises Small Office and Home Office (SOHO) TP-Link devices. Quad7 has been associated with the Chinese APT group Storm-0940, known for targeting organisations in North America and Europe. Storm-0940 gains initial access via valid credentials and then uses scanning and credential-dumping tools to move laterally within networks. The group installs proxy tools and remote access Trojans to maintain access and exfiltrate data. Storm-0940 typically gains initial access through valid credentials obtained via password-spraying operations.

Volt-Typhoon and KV-Botnet

In January, following a joint operation by the FBI and international law enforcement agencies, it was revealed that Volt-Typhoon, a Chinese state-sponsored threat group, was working to rebuild its KV-Botnet. The group focused on compromising SOHO networking devices in Asia, installing custom malware to stabilise proxy channels and maintain persistent access within compromised networks.

Socks5Systemz Botnet

Active since at least 2016, Socks5Systemz Botnet is believed to be part of the illegal proxy service Proxy.AM. Loaders such as SmokeLoader, PrivateLoader and Amadey distribute the Socks5Systemz malware. These loaders convert infected systems into Socks5 proxies that support further malicious activities.

Recommendations to Mitigate Risks

Based on the threats observed and analysed in this report, the Adarma Threat Intelligence Team recommend the following measures for all organisations to take to protect themselves against cyber threats and associated risks.

Implement a Cybersecurity Awareness Programme

Develop an effective cybersecurity awareness program for all staff, with a focus on recognising and responding to social engineering tactics such as spear phishing, phishing and vishing. These tactics remain the most common initial access tactics used against the technology sector.

Conduct a Cyber Risk Assessment

Perform a comprehensive cyber risk assessment of your organisation's network, devices, applications and users. This will help identify your current security controls, as well as any weaknesses or vulnerabilities that require remediation.

Patch Vulnerabilities

Regularly and appropriately patch vulnerabilities to reduce risks across your assets and applications. This includes addressing vulnerabilities in internet-facing systems and devices, which are common entry points for attackers.

Develop a Cyber Incident Response Plan

Create a detailed cyber incident response plan to enable quick and effective action in the event of an attack. This plan should outline the steps and procedures required to mitigate incidents and recover effectively. If your organisation is relying on the services of a third-party cybersecurity company, such as those provided by Adarma, ensure these are fully integrated into the plan.

Introduce Credential Monitoring

Implement a credential monitoring process to identify and address compromised credentials effectively. Stolen credentials are frequently advertised for sale on dark web forums and marketplaces, as highlighted in this report.

How Adarma Can Help

ADARMA
TOGETHER WE'VE GOT THIS

We are Adarma, the UK's leading security operations specialist for modern global enterprises. We protect organisations in the FTSE 350, including those in CNI and other regulated sectors. We offer effective threat detection and incident response, acting as an extension of your team to enhance your security posture and optimise security investments for maximum risk reduction.

Our security operations platform, Socket, along with our engineering expertise, provides co-managed security monitoring and consulting services, integrated with top enterprise security providers like Splunk, Google, and Microsoft. Our mission is to make cyber resilience a reality for organisations worldwide.

Our Services

ADARMA
TOGETHER WE'VE GOT THIS

Threat Intelligence Platform Management

Adarma's Threat Specialists can set up, configure, and maintain a threat intelligence platform tailored to your business needs. This platform enables the storage of reports, incident details, and indicators of compromise (IOCs) while integrating intelligence feeds into your SIEM, EDR, firewall, web proxy, or phishing protection solutions. By creating associations between threat actor groups, malware types, and related IOCs, the platform streamlines investigations and prioritises detection efforts.

Security Threat Modelling

Our services include security threat modelling that adheres to industry standards. We can assess threats for applications, platforms, or entire organisations, helping our customers in identifying potential vulnerabilities and risks that could affect their systems and solutions.

Quarterly Threat Briefings

To support your long-term strategic planning, our Threat Intelligence team provide quarterly threat briefings. These briefings focus on trends based on industry sector, geographical location, and other customer-specific considerations, providing senior stakeholders with the insights they need for effective planning, budgeting, and risk management.

ADARMA
TOGETHER WE'VE GOT THIS

Monthly Operational Briefings

To deliver actionable intelligence that informs short-term tactical decision-making and resource allocation, we provide monthly operational threat briefings. Our Threat Intelligence team monitors data sources, threat feeds, dark web tools, and information-sharing platforms to deliver detailed breakdowns of current and emerging security threats to your business.

Threat Hunting Expertise

Adarma's Threat Team comprises specialists and analysts experienced in threat hunting across SIEM and EDR platforms. We conduct custom behavioural threat hunts, tailored to your organisation's unique security concerns. These hunts uncover previously undetected malicious activity, logging issues, compliance problems, and offer recommendations to enhance your security posture.

Credential Monitoring Service

Adarma's Threat Specialists can set up monitoring for compromised credentials relating to your organisation. Compromised credentials are a valuable asset for cybercriminals to enable initial access to networks and resources. This service provides the ability for Adarma to respond and mitigate the risks when compromised credentials are identified in dark web forums,
chat services and marketplaces used by cybercriminals.

Get in touch

If you would like to speak to an Adarma consultant about any issue or approaches raised in this report, please contact us at **hello@adarma.com**.

ADARMA
TOGETHER WE'VE GOT THIS

hello@adarma.com

www.adarma.com