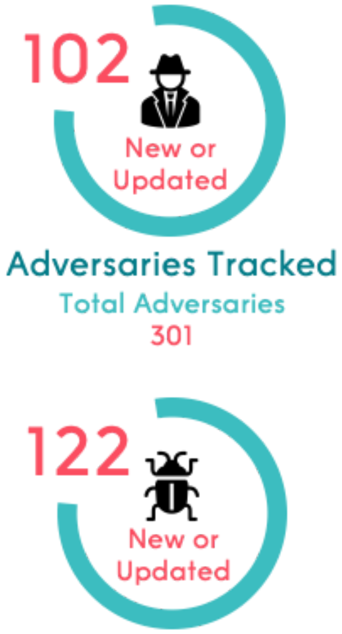
ADARMA
TOGETHER WE'VE GOT THIS

THREAT LANDSCAPE REPORT: HIGHLIGHTS

Q4 2024

Threat Landscape Overview – Q4 2024

Adarma's Q4 2024 Threat Landscape report, compiled by Adarma's Threat Intelligence team, presents a comprehensive analysis of the most significant cyber threats faced by businesses globally. It provides an in-depth look at ongoing and emerging cyber threats, drawn from both internal and external data sources, including insights from Adarma's Security Operations Centre (SOC) and partner, Recorded Future.



102
New or Updated
Adversaries Tracked
Total Adversaries
301

122
New or Updated

Figure 1 – The image above shows adversaries and malware tracked by Adarma's threat intelligence team. These statistics are based on intelligence obtained and information ingested and tracked in the Threat Intelligence Platform (TIP) in the quarter.

Active Threat Landscape at a Glance

Ransomware: A Persistent Threat Across Industries

Over the course of this quarter, ransomware continued to dominate the cyber threat landscape, with significant activities from well-established groups, as well as the rise of new ransomware actors.

In addition to ransomware, nation-state groups and hacktivists remained active, exploiting vulnerabilities in various industries, particularly healthcare, aviation, and critical national infrastructure (CNI).

New players like Cicada3301, which emerged in late June 2024, were observed targeting VMware ESXI servers, utilising similar techniques to the now-defunct BlackCat ransomware group. The overlap of these features might indicate that Cicada3310 is likely a rebrand of the now-defunct BlackCat ransomware group. Their focus on both Linux and Windows operating systems poses a growing threat to enterprise environments. Notably, ransomware groups like BianLian and Rhysida were observed leveraging Microsoft Azure tools, such as Azure Storage Explorer and AzCopy, to exfiltrate data, taking advantage of trusted services to bypass traditional detection mechanisms.
Based on the intelligence gathered throughout Q3 of 2024, the ransomware groups highlighted in figure 2 have been the most active on their respective leak sites.

Trends from the Trenches

Ransom Hub

One of the most active ransomware-as-a-service (RaaS) groups, RansomHub continued to expand its global presence, with a particular focus on industries such as healthcare, aviation, and retail. Their attacks, including the breach on Malaysia's Prasarana public transport network and several healthcare providers in the UK and US, demonstrate their increasing capability and adaptability.

A joint advisory published by CISA (Cybersecurity and Infrastructure Security Agency) on August 29, 2024, highlighted RansomHub's success as a service model, attracting high-profile affiliates from other ransomware variants such as Lockbit and ALPHV, further cementing its reputation in the cybercriminal ecosystem.

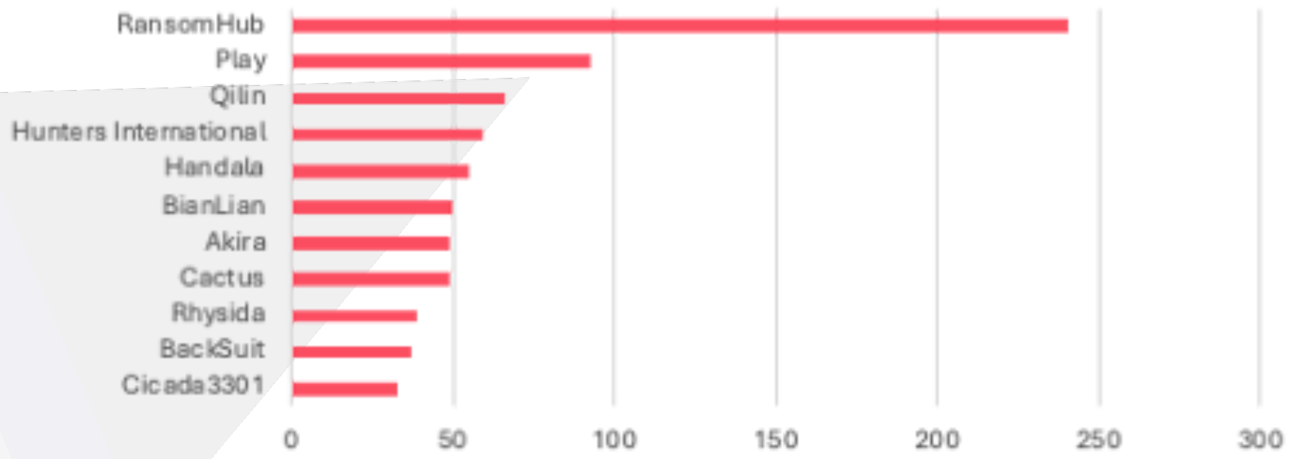


Figure 2 — The graph above shows the most active ransomware groups in Q3 of 2024

Play

Also known as PlayCrypt, was responsible for several significant ransomware attacks in Q3 2024. Notable incidents include an attack on the Texas Electric Cooperatives Inc between July 21-25, 2024, stealing personally identifiable information (PII), including names, Social Security numbers, and driver's license numbers.

The group also targeted the Hayden Power Group a Pennsylvania-based electrical contractor, compromising sensitive data such as client documents, payroll records, tax information, and financial data. Then in August 2024, Play targeted Microchip Technology Inc, a semiconductor manufacturer, stealing employee information and causing disruptions to its operations.

Qilin

was highly active in data exfiltration and service disruption across various industries. They were also observed collaborating with Scattered Spider (aka Octo Tempest), deploying ransomware samples with a focus on VMware ESXI servers. This activity highlights the group's growing technical prowess and ability to exploit vulnerabilities across both Linux and Windows environments.

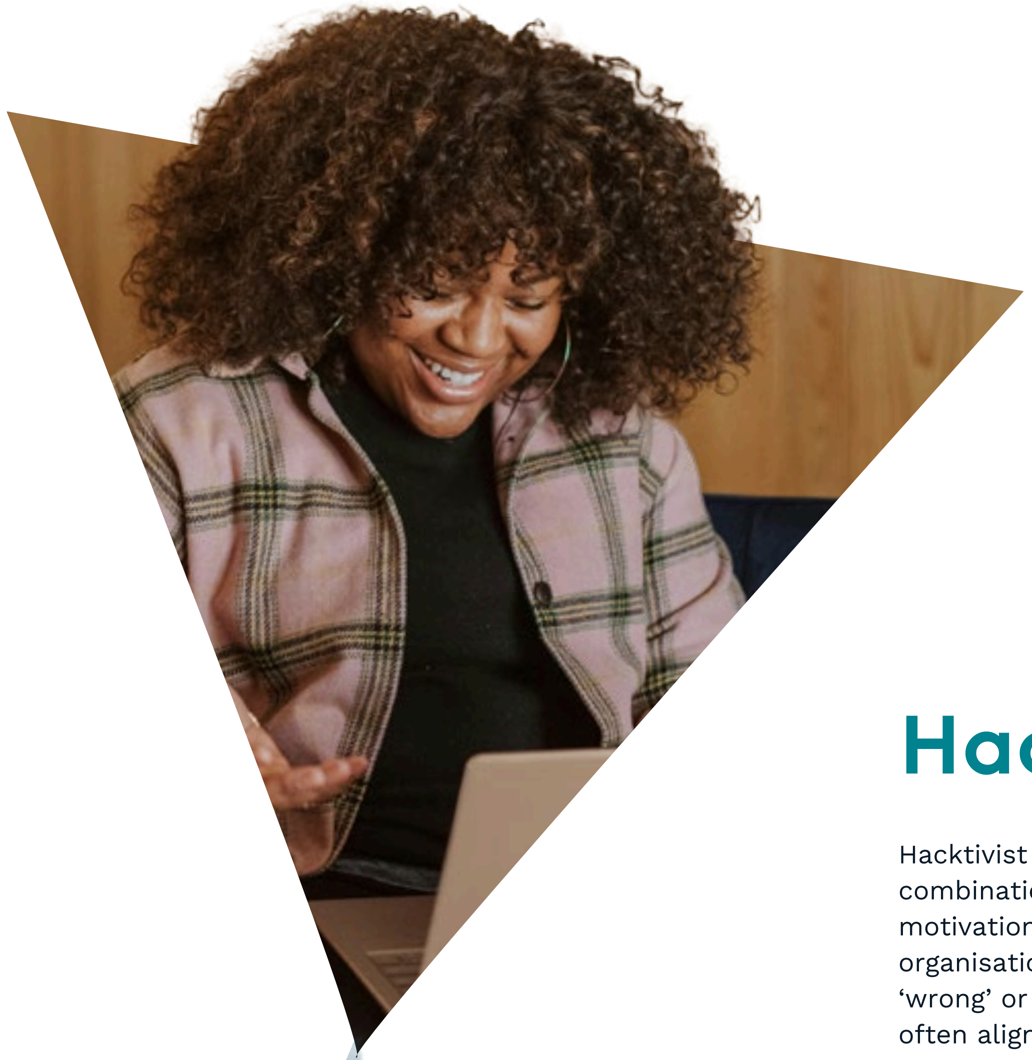
Regulatory Developments in the UK

In response to the increasing prevalence of ransomware attacks on businesses and organisations in the UK, the government has taken steps to strengthen its cybersecurity regulations.

A Cyber Security and Resilience Bill was announced, designed to bolster protections for digital services and supply chains.

The proposed law will introduce mandatory reporting requirements for companies that fall victim to ransomware attacks, ensuring greater transparency and faster response to such incidents. The impact of this new law will primarily focus on regulated entities, rather than imposing blanket rules across the private sector. By targeting the most critical areas of the economy, the government aims to mitigate the far-reaching consequences of ransomware.

Additionally, the UK plans to designate the data centre sector as part of its CNI. This sector's inclusion under CNI will ensure that incidents involving data centres receive heightened attention and response. This new categorisation will cover data deemed vital to national interests, such as NHS information, financial records, and personal smartphone data. The Cyber Security and Resilience Bill, which is expected to pass later this year, will integrate these changes to better protect key digital assets across the country.



Hacktivism

Hacktivist activities are typically driven by a combination of political, ideological, or social motivations, with groups targeting organisations they perceive as engaging in 'wrong' or 'unjust' actions. These campaigns often align with political or geopolitical issues, revenge, or protest, and aim to disrupt or damage companies or organisations that oppose their moral standpoint.

Historically, common tactics employed by hacktivists include website defacements and Distributed Denial of Service (DDoS) attacks. However, it has been reported that since Russia's invasion of Ukraine, there has been a noticeable shift in how hacktivism is being conducted.

In Q3, hacktivist groups have displayed increased coordination, strategic planning, and closer alignment with state-sponsored interests. This has blurred the traditional lines between hacktivism, cybercrime, and state-sponsored activities. One of the more significant developments during this period is the growing trend of hacktivist groups adopting ransomware as a means of funding future operations.

Notable Hacktivist Activity

KillSec, a pro-Russian group, has launched its own RaaS operation, expanding its cyber arsenal. Similarly, AzzaSec, an Italian-based group aligned with Russian interests, released a custom-built ransomware targeting Windows systems. Meanwhile, the pro-Ukrainian hacktivist group Head Mare has also deployed ransomware attacks, specifically targeting organisations within Russia and Belarus.

Head Mare is reported to use leaked versions of well-known encryptors such as Lockbit and Babuk, but it distinguishes itself from other hacktivist groups by utilising its own custom malware to gain initial access. Its tools, PhantomDll and PhantomCore, are delivered through phishing campaigns aimed at sectors such as transportation, energy, manufacturing, entertainment, and government organisations.

This approach is increasingly common, as state-sponsored groups like Chamelgang, Andariel, and Moonstone Sleet have previously leveraged ransomware in cyber operations. In a notable example of the growing strategic nature of hacktivism, the Cyber Army of Russia Reborn (CARR) has actively targeted CNI in the United States and Europe. This escalated to the point where, on July 19, 2024, the US imposed sanctions on two members of the group for their cyber activities. Despite Russia's embassy labelling these sanctions as "propaganda," CARR took to their Telegram channel to celebrate the sanctions as a form of recognition for their efforts.

Further enforcement actions in Q3 2024 saw the arrest of three members of NoName057(16), a pro-Russian group, by Spanish police in late July. These arrests reflect the growing international response to the evolving and increasingly sophisticated nature of hacktivist campaigns, signaling an ongoing battle between law enforcement agencies and politically motivated cyber actors.

Emerging Threats

Defence Evasion – Endpoint Detection and Response Killing tools

In recent years, threat actors have increasingly developed and deployed tools designed to disable Endpoint Detection and Response (EDR) systems during cyberattacks. These tools serve a dual purpose: evading detection and generating financial profit, as they are often sold on underground marketplaces.

During Q3 of 2024, there was a noticeable rise in the use and sale of custom EDR tools aimed at disabling EDR software. SentinelLabs reported in July 2024 that FIN7, a notorious Russian threat group known for its financial fraud operations and ransomware deployments, had been advertising a tool called AvNeutralizer.

This custom tool, which has been circulating in underground marketplaces since at least 2022, received upgrades allowing it to disrupt protected system processes in EDR software, resulting in a Denial-of-Service (DoS) condition. By rendering the EDR system inoperable, AvNeutralizer helps threat actors execute their attacks undetected.

RansomHub has been observed utilising a different EDR-disabling tool named EDRKillShifter. Unlike AvNeutralizer, which causes a DoS, EDRKillShifter exploits a Bring Your Own Vulnerable Driver (BYOVD) vulnerability to escalate privileges. This allows attackers to deactivate EDR software without triggering system failures, giving them more control over the targeted environment.

In other attacks linked to RansomHub, threat actors have deployed Poortry, an EDR-killing tool with capabilities similar to wiper malware. Poortry not only disables the EDR system but also ensures it cannot be restarted by deleting key executable files, dynamic link libraries (DLLs), and other critical components. This aggressive approach makes defence evasion highly effective and leaves security teams with limited recovery options during the attack.

The rise in the availability and sophistication of these EDR-killing tools underscores the increasing importance of developing more resilient detection and defence systems to counteract these emerging threats.

> **“EDR killing tools significantly threaten companies worldwide. Whenever possible, constant monitoring of unusual process termination or suspension should be considered, particularly if these are related to EDR solutions.”**

Credential Access - Browser in Kiosk Mode

In Q3 of 2024, a novel technique emerged that leveraged Amadey malware and an AutoIt script to deceive victims into entering their credentials into a browser locked in “Kiosk Mode.” Once the Amadey Loader is deployed on a victim’s system, it loads two key components: the StealC info-stealer and a Credential Flusher implemented through an AutoIt script.

This script forces the victim’s browser into kiosk mode, while simultaneously disabling critical keyboard functions like ESC and F11, which would normally allow users to exit the mode. The victim is tricked into believing that the only way to close the window is by entering their credentials into the browser.

However, once the credentials are entered, the StealC malware accesses the browser’s credential store on the disk and exfiltrates the stored credentials to the threat actor's Command and Control (C2) infrastructure. This technique illustrates how cybercriminals can use simple yet effective deception tactics to trick users into revealing their credentials.

> **“Remaining calm is crucial when the system does not behave as expected, particularly if important information is requested via browser applications. Always contact your IT department and inform them of the situation when in doubt.”**

Data Exfiltration and Ransomware - BazaCall Campaign

Fraudulent call centres, known for their social engineering tactics, are increasingly being used to launch sophisticated cyber campaigns aimed at financial gain. In Q3 of 2024, Microsoft released an analysis of a campaign that employed call centres to trick victims into downloading malware designed for data exfiltration and ransomware deployment.

The campaign involved sending victims an email notifying them of a supposed subscription charge, urging them to call a provided phone number to resolve the issue. By using this method, the attackers were able to bypass traditional phishing and malware detection systems, as no malicious attachments or links were involved.

Once the victim contacted the call centre, an operator instructed them to download BazarLoader, also known as BazarBackdoor, a loader malware that provides backdoor access to the victim's device and enables the download of additional malicious payloads. According to Microsoft, the threat actors were able to exfiltrate data and deploy ransomware within 48 hours of the initial compromise.

BazarLoader, known for its stealthy operations, allows threat actors to maintain remote control over the compromised system, leading to further data breaches and potential ransomware attacks. This campaign highlights the evolving tactics of cybercriminals, who are now using legitimate-seeming processes like call centres to sidestep conventional cybersecurity defences and execute damaging cyber operations.

How Adarma Can Help

We are Adarma, the UK's leading Security Operations specialist for modern global enterprises. We protect organisations in the FTSE 350, including those in Critical National Infrastructure 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

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.

Monthly Operational Briefings

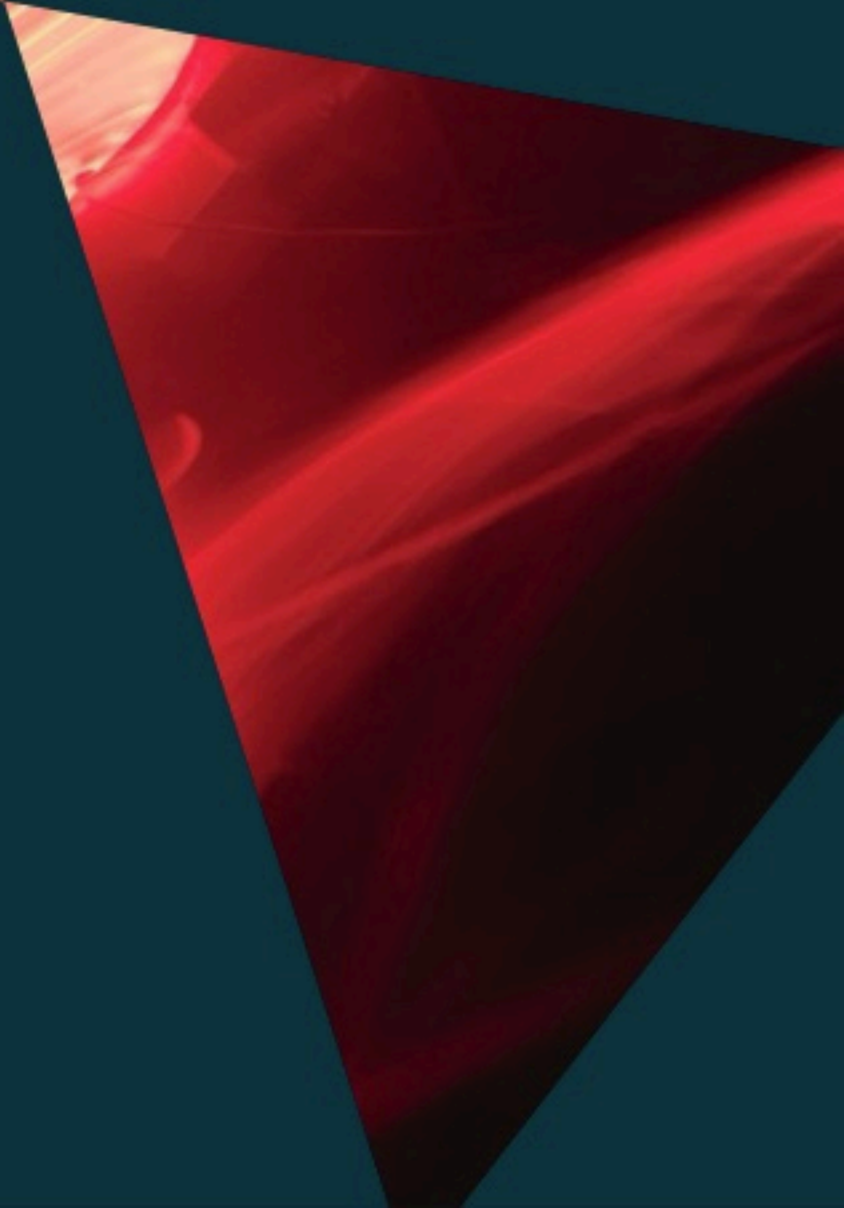
To deliver actionable intelligence that informs short-term tactical decision-making and resource allocation, we provide monthly operational threat briefings. Our Threat Intelligence team monitors data sources, threat feeds, dark web tools, and information-sharing platforms to deliver detailed breakdowns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

Get in touch

If you would like to speak to our Threat Intelligence team please email hello@adarma.com.



ADARMA

TOGETHER WE'VE GOT THIS

hello@adarma.com

www.adarma.com