ADARMA

TOGETHER WE'VE GOT THIS

FINANCIAL SERVICES THREAT LANDSCAPE REPORT

Q4 2024

Contents

ADARMA
TOGETHER WE'VE GOT THIS

Purpose 03

Insights from Adarma 04

Significant Cyberattacks in Q3 2024 06

APT Activity Targeting Financial Services 07

Prevalent ATT&CK Techniques 08

How Adarma Can Help 10

Our Services 11

Purpose

The Adarma Q4 Financial Services Threat Landscape Report delivers a detailed analysis of the key cyber threats that impacted the sector from July to September 2024.

Drawing on observations and research by Adarma's Threat Intelligence Team and partners such as Recorded Future, this report highlights the most significant cyber activities during that period. While primarily focused on Q3, critical insights outside of this timeframe have been included to provide a more complete picture of evolving threats.

102

out of 301

New or Updated

Adversaries Tracked

122

out of 340

New or Updated

Malware Strains Tracked

This figure shows the number of adversaries and malware strains tracked by the Adarma Threat Intelligence Team in Q3 2024.

Insights from Adarma

The financial services sector remains one of the most targeted industries, attracting various cybercriminals due to the substantial volumes of sensitive data it handles.

In Q3 2024, financially motivated attackers, especially those deploying banking trojans and Advanced Persistent Threat (APT) groups, shaped much of the threat landscape. Adarma's Threat Intelligence Team observed a significant increase in Android malware, more sophisticated banking trojan variants, and a notable shift in adversaries' focus toward cloud-based financial infrastructure.

Banking Trojans

Banking trojans, a type of malware that steals financial data by mimicking legitimate banking apps, emerged as a serious risk to financial institutions globally. In Q3, three trojans stood out within the threat landscape; NGate, Octo2, and TrickMo.

NGate

NGate is a new Android malware strain recently used to steal financial data from three Czech banks. What sets this trojan apart is its ability to intercept payment card data through a malicious app on a victim's Android device. By exploiting near field communication (NFC), the trojan relays data from the victim's physical payment cards directly to the attacker's device. This enables attackers to use the stolen data for ATM withdrawals and, if unsuccessful, transfer funds directly from the victim's bank account. This advanced technique marks a significant evolution in banking trojans.

Octo2

In Q3, a new version of the Octo Android malware, known as Octo2, emerged. This update disguises itself as legitimate apps like NordVPN, Google Chrome, and Europe Enterprise to evade detection. Octo2 has been enhanced with greater operational stability, sophisticated anti-analysis and anti-detection capabilities, and a domain generation algorithm (DGA) to maintain resilient command and control (C2) communications. Current Octo2 campaigns are focused on Italy, Poland, Moldova, and Hungary. Given that the Octo Malware-as-a-Service (MaaS) platform has previously been used to target regions such as the U.S., Canada, Australia, and the Middle East, it is likely that Octo2 will soon expand to other areas as well.

TrickMo

A more advanced version of the TrickMo Android banking trojan, believed to be created by the now defunct TrickBot cybercrime group, has recently surfaced. This updated variant includes enhanced anti-analysis features and the ability to display fake login screens to steal banking credentials. Disguised as the Google Chrome browser, the trojan prompts victims to "update Google Play Services" upon launch, encouraging them to click "Confirm." If the user follows this prompt, an APK file containing the TrickMo payload is downloaded under the name "Google Services," after which the victim is instructed to enable accessibility services for the app. TrickMo's new capabilities include screen recording, keystroke logging, photo and SMS harvesting, remote device control for on-device fraud (ODF), and leveraging Android's accessibility services to execute HTML overlay attacks, perform clicks, and mimic gestures on the device.

Significant Cyberattacks in Q3 2024

ADARMA
TOGETHER WE'VE GOT THIS

Several major breaches were disclosed in Q3, which underscore the vulnerabilities in the financial services sector.

JULY

01

In July, Evolve Bank & Trust disclosed in a filing with Maine's attorney general that the personal data of more than 7.6 million of its customers was stolen during a LockBit phishing attack in late May. At least three of the bank's major partners were impacted by the attack, including Wise, a partner that had severed ties with Evolve the previous year. According to the bank, LockBit had released the stolen data, including Personal Identification Information (PII), on the dark web. This attack highlights the ongoing challenges posed by phishing campaigns as an entry vector for ransomware groups like LockBit.

AUGUST

02

In late August, California-based credit union Patelco, a prominent financial institution, informed US regulators of a June 29 cyberattack that exposed sensitive information, including names, dates of birth, social security numbers, and driver's license numbers of 726,000 customers. It is suspected that attackers had gained access to Patelco's networks as early as May 23. The ransomware group RansomHub claimed responsibility, executing the attack strategically before the July 4 holiday to maximise disruption. Frustrated customers reported on Facebook that they were restricted to withdrawing only $500 from ATMs. This incident reflects how attackers are becoming more strategic in how and when they target victims for maximum impact.

SEPTEMBER

03

In a notification letter filed September 6 with regulators, Slim CD, a Florida-based electronic payment processing company, disclosed that credit card information of nearly 1.7 million people was exposed in a cyberattack that took place in mid-June. An internal investigation revealed that an unidentified threat actor had access to company systems as early as August 2023, but the actual data breach did not occur until June 14, 2024. This attack emphasises the importance of strong detection measures to avoid attackers squatting long-term undetected in networks.

APT Activity Targeting Financial Services

Advanced Persistent Threats (APTs) continued their campaigns against the financial services sector in Q3, with two groups standing out.

Scattered Spider

Noted for targeting cloud infrastructure, Scattered Spider employs sophisticated social engineering techniques and exploits weak identity administration processes. Their ability to bypass cloud defences, particularly by creating unauthorised virtual machines (VMs) in environments like Microsoft Azure and Amazon Web Services (AWS), is especially concerning for organisations relying on cloud services.

The group also uses phone-based social engineering techniques to manipulate their targets, mainly employees working in IT service desks and identity administration. Throughout the campaigns, the actors have employed phishing pages that prompt the victim into entering company information such as employee IDs and manager names to help in their social-engineering activities; these especially come in handy when attackers impersonate employees during voice phishing calls.

Another method of initial access used by this group is looking for authentication token leakage on publicly exposed code repositories like GitHub. Once inside a compromised user account, the group targets cloud infrastructure like Microsoft's Azure or AWS instances and, in some cases, creates unauthorised virtual machines (VMs) that bypass the victim's security systems since new machines commonly do not come with security tools pre-installed.

BlindEagle (APT-C-36)

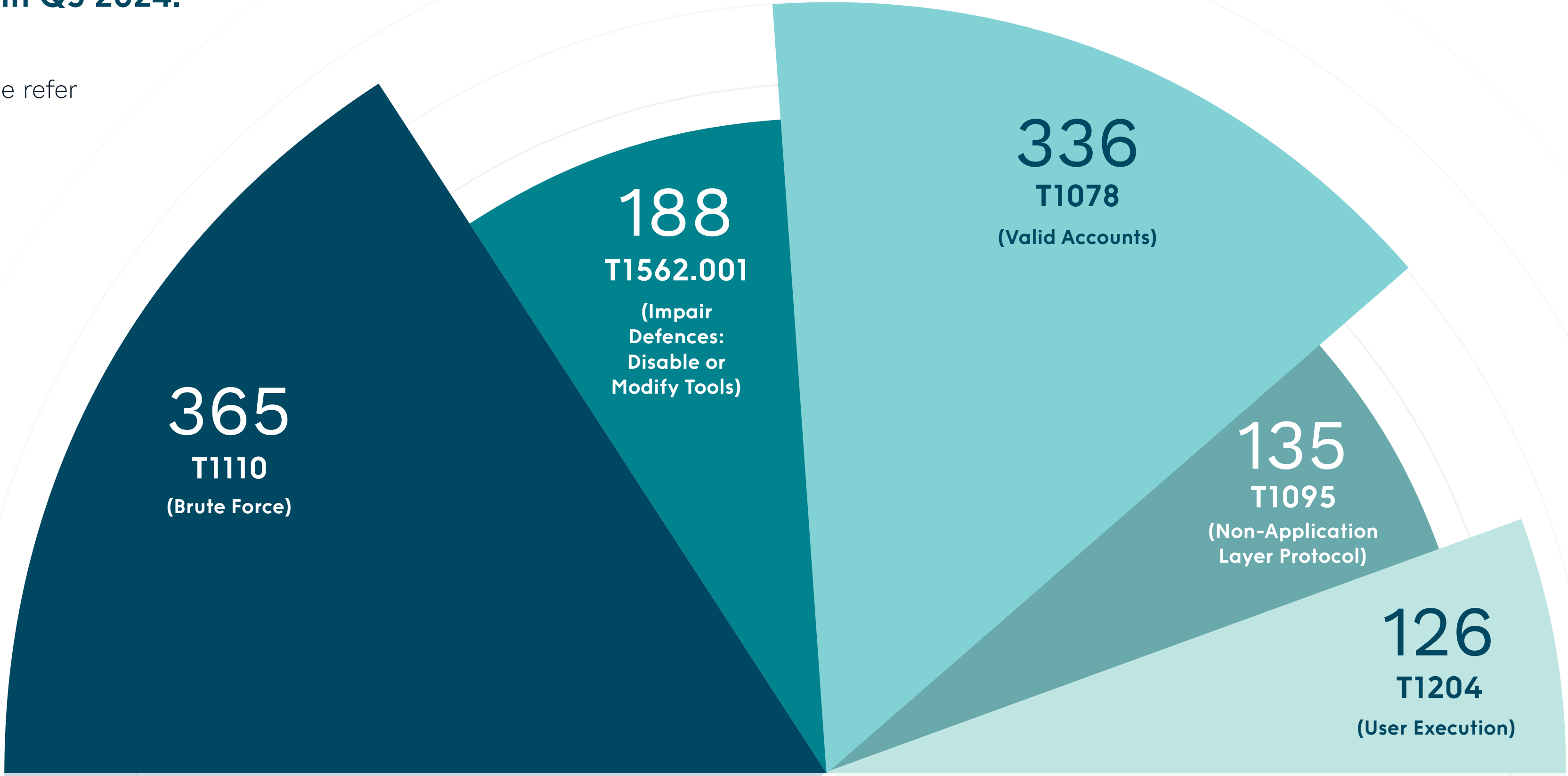
This Latin American group frequently targets Critical National Infrastructure (CNI) using phishing emails tailored to specific sectors, e.g. government or financial institutions. The phishing links direct the victim to an actor-controlled site that determines what country they are from, and if it is in the target country list, an initial dropper is downloaded. Their campaigns involve multi-stage payloads, typically distributed through platforms like Pastebin, GitHub and Discord, enabling them to maintain a presence in compromised environments.

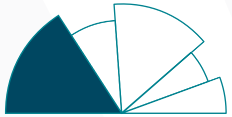
Prevalent ATT&CK Techniques

Top attack techniques discovered by Adarma's internal SOC analysts while responding to incidents targeting the financial services industry in Q3 2024.

For detailed information about these techniques, please refer to the Mitre ATT&CK website (https://attack.mitre.org/).

> **Brute force attacks ranked top in investigated incidents, highlighting the need for stronger authentication practices."**
>
> Adarma Threat Intelligence Team

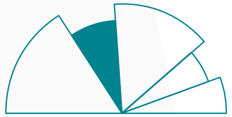




T1110

Brute Force

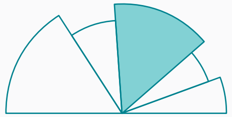
Adversaries attempt to exploit credentials obtained from breach dumps to access target accounts through credential reuse. Users often use the same passwords across different personal and business accounts, making this tactic effective. Credential stuffing involves using these username and password combinations to try and gain access, but it carries risks such as triggering account lockouts or numerous authentication failures, depending on the organisation's policies.



T1562.001

Impair Defences: Disable or Modify Tools

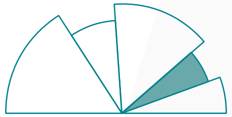
This involves attackers disabling or altering security tools to evade detection. This can include stopping antivirus software, modifying registry keys, or disabling logging features to avoid raising alerts. By tampering with these defences, adversaries can operate undetected and prolong their access within a network.



T1078

Valid Accounts

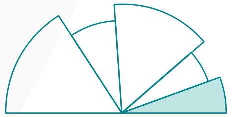
Adversaries abuse compromised account credentials to gain Initial Access, Persistence, Privilege Escalation, or Defence Evasion. These credentials can bypass system access controls, allowing persistent access to remote systems and services like VPNs, Outlook Web Access, and remote desktops. Additionally, compromised credentials can grant higher privileges or access to restricted network areas. Adversaries may also avoid using malware or tools to make detection more difficult.



T1095

Non-Application Layer Protocol

This technique is used by attackers to communicate covertly using lower-layer protocols like ICMP or UDP, bypassing detection focused on standard application-layer protocols like HTTP. This tactic allows the attackers to maintain a C2 channel that can evade traditional monitoring, as these protocols are less scrutinised on most networks.



T1204

User Execution

This attack involves tricking users into running malicious content, often via phishing or social engineering. Adversaries use malicious links (T1204.001) or files (T1204.002), like infected documents or executables, to lure users into initiating malware. Sometimes, they embed malicious scripts within images (T1204.003), which execute upon interaction. This approach is commonly used for initial access, targeting human vulnerabilities. Defences include training users to identify phishing, endpoint protection, and filtering tools to block harmful content.

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 highly-regulated sectors. We offer effective threat detection and incident response, acting as an extension of your team to enhance your security posture and optimise your 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 Intelligence Team 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 Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), firewall, web proxy, or phishing protection solutions. The platform streamlines investigations and prioritises detection efforts by creating associations between threat actor groups, malware types, and related IOCs.

Security Threat Modelling

Our threat specialists conduct security threat modelling that meets industry standards. We can assess threats for applications, platforms, or entire organisations, helping our customers identify potential vulnerabilities and risks that could affect their systems and solutions.

Quarterly Threat Briefings

Our Threat Intelligence Team provides quarterly threat briefings to support your long-term strategic planning. 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

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

Threat Hunting Expertise

Adarma's Threat Intelligence 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, and compliance problems and offer recommendations to enhance your security posture.

In conjunction with Adarma's security consultants, the Threat Intelligence Team assist in building and running cybersecurity crisis tabletop simulations based on current threats as seen in the wild, providing your stakeholders with real-world preparedness.

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