ADARMA
TOGETHER WE'VE GOT THIS

RETAIL THREAT LANDSCAPE REPORT

Q3 2024

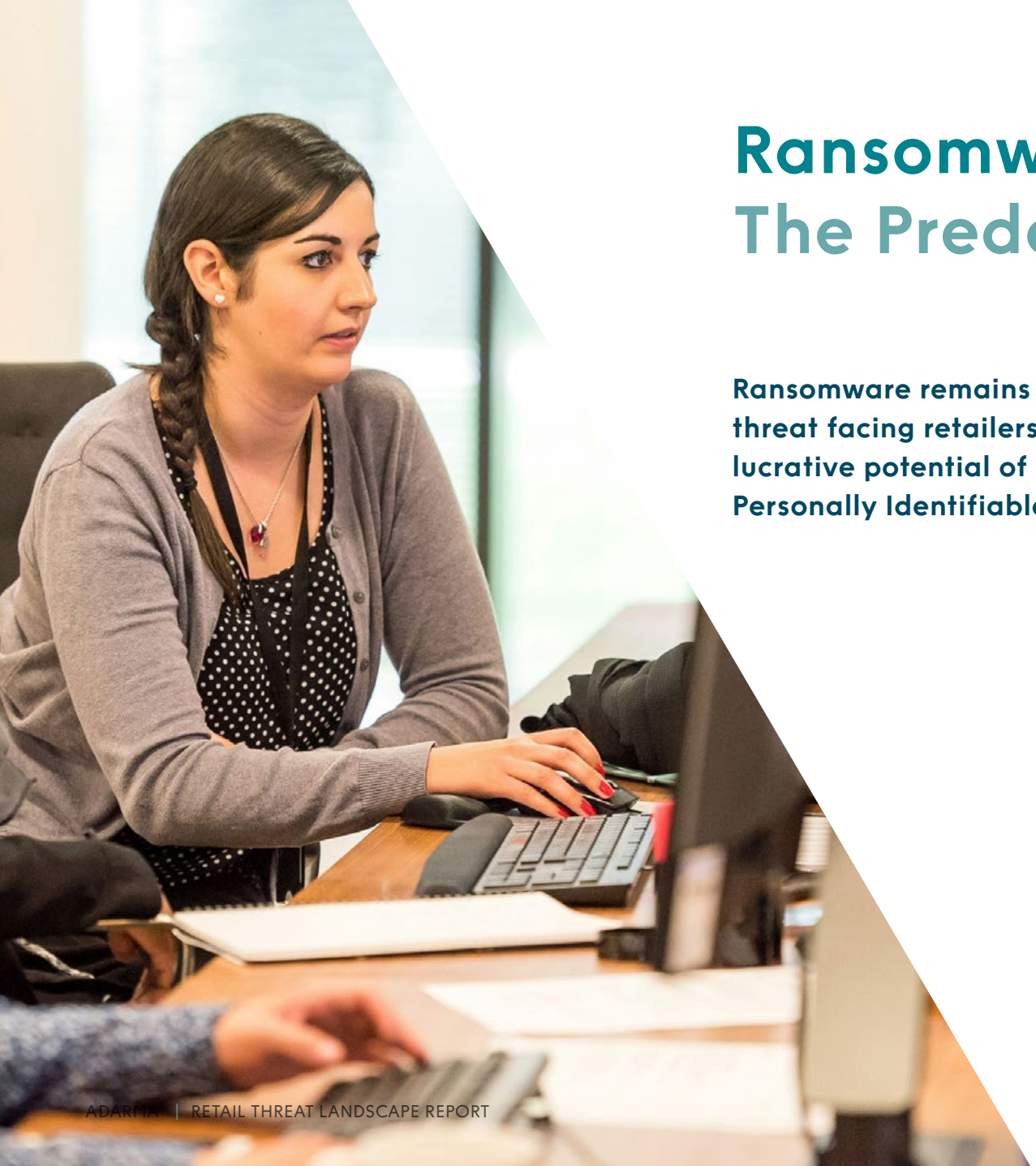
Contents

ADARMA

Understanding the Retail Cyber Threat Landscape: Insights from Adarma

The retail industry has long been a prime target for cybercriminals, and Adarma's Q2 2024 Threat Landscape Report reinforces this trend.

Drawing on intelligence from internal and external sources, including Adarma's Security Operations Centre (SOC) and their partner Recorded Future, this report sheds light on the evolving Tactics, Techniques, and Procedures (TTPs) currently impacting the retail sector.



Ransomware Attacks:
The Predominant Threat

Ransomware remains the most significant threat facing retailers, driven by the lucrative potential of payment data and Personally Identifiable Information (PII).

The report highlights that ransomware groups are increasingly employing double extortion tactics—encrypting data and threatening to leak it unless the ransom is paid. This method has seen widespread adoption across the sector, with multiple groups such as LockBit, Black Basta, and Hunters International at the forefront.

LockBit, for instance, have been particularly active, claiming attacks on retailers across multiple countries including Canada, the US, and New Zealand. The case of London Drugs, a Canadian healthcare retailer, stands out where the company refused to meet the ransom demand. In retaliation, the attackers released portions of the stolen data. This incident not only underscores the operational disruption caused by such attacks but also highlights the reputational risks involved when companies choose not to comply with ransom demands.

Data Breaches: A Growing Concern

The retail sector also saw a significant number of data breaches often linked to vulnerabilities in third-party services.

Notably, the breach of Snowflake, a cloud data storage provider, had a cascading effect on multiple retailers including Neiman Marcus and Advance Auto Parts. This breach underscores the risk posed by supply chain vulnerabilities and the potential for widespread impact when a single provider is compromised.

Threat actors like IntelBroker have been particularly active, claiming responsibility for several high-profile breaches. For example, the UK retailer ShoeZone had data from 200,000 individuals compromised, including sensitive information like credit card details. These breaches not only expose the immediate victims but also highlight the ongoing risk to customer trust and the potential for regulatory penalties.

Phishing and Smishing

Phishing and smishing (SMS phishing) campaigns remain a persistent threat, with the group Storm-0539, also known as Atlas Lion, particularly targeting US retailers.

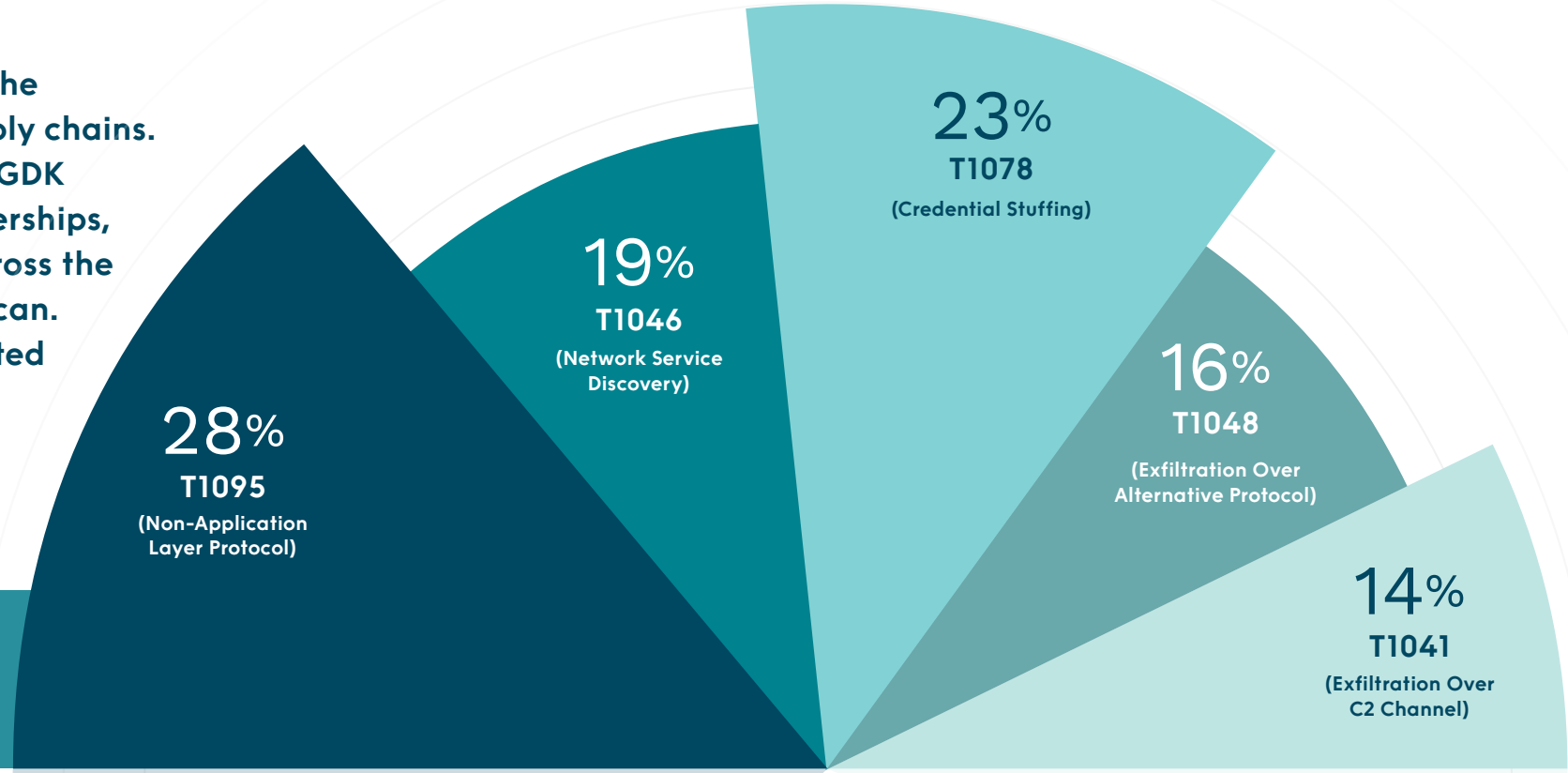
These attacks are often aimed at committing gift card fraud, where the attackers use phishing tactics or compromised accounts to steal credentials and bypass multi-factor authentication, granting them long-term access to corporate networks.

The tactics employed by Storm-0539 illustrate the evolving sophistication of social engineering attacks and their effectiveness in compromising even well-defended organisations. It's worth noting that gift card fraud can also involve attempts by attackers to trick individuals or businesses into purchasing and sending gift cards or to reveal gift card codes.

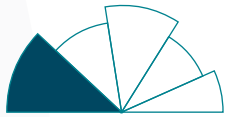
Supply Chain Vulnerabilities and Broader Impacts

Ransomware's impact extends beyond the immediate victims to their broader supply chains. This is evidenced in the June attack on GDK Global, a software provider to car dealerships, which led to widespread disruptions across the automotive retail sector in North American. This incident highlights the interconnected nature of modern retail operations and the systemic risks posed by attacks on key service providers.

The top techniques identified in incidents concerning the Retail sector that Adarma's internal SOC analysts addressed with in Q2 of 2024.



If you would like further information about specific Enterprise ATT&CK techniques, please refer to the Mitre website.



T1095

Non-Application Layer Protocol

When an adversary uses an OSI non-application layer protocol for communication between a host and a C2 server or among infected hosts within a network. They may use network layer protocols like ICMP, transport layer protocols like UDP, session layer protocols like SOCKS, or redirected/ tunneled protocols like Serial over LAN (SOL). The list of potential protocols is extensive.

T1046

Network Service Discovery

When an adversary attempts to list services running on remote hosts and local network devices, especially those vulnerable to remote exploitation. They often use port or vulnerability scans, leveraging tools brought onto the system to gather this information.

T1078

Credential Stuffing

When an adversary obtains and abuses credentials of existing accounts to gain Initial Access, Persistence, Privilege Escalation, or Defence Evasion. They can use compromised credentials to bypass access controls on network resources, gain persistent access to remote systems and external services like VPNs, Outlook Web Access, and remote desktop, and escalate privileges or access restricted network areas.

T1048

Exfiltration Over Alternative Protocol

When adversaries steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

T1041

Exfiltration Over C2 Channel:

Adversaries steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Recommendations

Given the prevalence of ransomware, data breaches, and phishing campaigns, it's important for companies to prioritise network backups and software updates to prevent potential breaches.

Regular cybersecurity awareness training should be implemented for employees to educate them about the dangers of phishing attacks and to improve password security. It's also crucial to enhance endpoint security. Retailers must stay vigilant and proactive in their defences.

The growing complexity of these cyber-attacks, combined with the widespread impact of supply chain vulnerabilities, underscores the importance for organisations to assess their IT assets and technologies in order to establish a strong cybersecurity strategy. This strategy should include clearly defined policies and procedures outlining the necessary steps to be taken in the event of a security threat.

Implementing strong security measures and having a comprehensive incident response plan is more crucial than ever. For guidance on how to build a comprehensive incident response plan, please see our detailed checklist.

We Are Adarma

Adarma provides customised cybersecurity solutions to assist businesses in achieving future-ready cyber resilience. Our approach enables organisations to decrease cyber risks by implementing effective threat intelligence, exposure management, and detection and response capabilities.

Our expertise guarantees a balanced approach between security and operational efficiency, safeguarding our customers' most crucial infrastructure and data.

Discover our tailored services and find out why we are the preferred security partner for FTSE 350 firms.

Get in touch

If you would like to speak to an Adarma consultant about any issues or approaches raised in this paper, please email **hello@adarma.com**.

You may also be interested in our "How to Design a Future-Ready Security Operations Centre (SOC)" report. This report lays out a detailed blueprint for building a SOC that tackles today's challenges while anticipating and preparing for tomorrow's threats.

Scan the QR code to find out more.

ADARMA
TOGETHER WE'VE GOT THIS

hello@adarma.com

www.adarma.com