Demystifying Ransomware for Retailers

Harness the Power of Data Protection

Ward off the Dark Arts

As a retailer, you process troves of credit card transactions, and if you have a robust online marketplace or loyalty app, then you have access to your customers' personally identifiable information (PII). Therefore, it's no surprise that you're a favorite target for malicious actors and one of their preferred dark arts attack vectors, ransomware.

69% **In fact, 69% of retail organizations were hit by ransomware in 2023.[1]**

$2,458,481 **From a monetary perspective, retailers struck by ransomware are likely to pay a fortune, as the global mean ransom payment by retailers in 2023 was $2,458,481.[2]**

Like hexes, ransomware attacks can result in profoundly destructive and lingering consequences for retailers. The attack can result in reputational damage, loss of revenue from interrupted and suboptimal operations, potentially expensive compliance violations, detrimental strain upon relationships with vendors, suppliers, and partners, and even employee layoffs.

37% **It's reported that 37% of organizations were forced to eliminate jobs following a ransomware attack.[3]**

Ransomware Hex | Risks | Attack Anatomy | Protection | SageNet Effect | MNSP

Why Retailers Are at Risk of Ransomware

There are a myriad of reasons why retailers are susceptible to ransomware attacks, including:

1 Retailers collect and transfer scores of PII and financial information, making them a treasure trove for malicious extraction and extortion.

In January 2023, a leading sports and apparel retailer reported that the personal and financial information of 10 million customers was potentially accessed by hackers that targeted their online orders between November 2018 and October 2020.[4]

2 A compromised digital ecosystem can provide hackers access to launch further attacks across an organization's network and potentially, even third-party partner systems.

3 Many retailers' revenue can be seasonally dependent (from selling skis to Halloween costumes), and thus, attackers believe they're more than likely to pay a ransom if an attack coincides with the business' busy period. It's no surprise that the holiday shopping season is an active time for cyber criminals.[5]

4 The emergence and proliferation of IoT devices, in-store applications, and digital signage throughout retail businesses create a larger attack surface.

5 Many retailers rely upon complex supply chains and just-in-time deliveries, which opens an ample array of auxiliary targets for attackers.

6 From cashiers and stockers to bookkeepers and brand ambassadors, a retailer's staff may be naive about cybersecurity best practices and, thus, be potentially easy pickings for phishing attacks.

In April 2023, a US-based payments processor was hit by a ransomware attack that caused a data center outage that disrupted some of their digital services, including POS systems and back-office applications. As a result, users were unable to set staff schedules, process payroll, or accept loyalty points and gift cards.[6]

Anatomy of a Retail Ransomware Attack

1

Payload

An employee opens a malicious link or email attachment, or is hit by a drive-by download from a compromised website.

2

Execution

Malicious code executes and contacts a command-and-control server for instructions.

3

Lateral Movement

The malware moves to steal credentials, escalate privileges, and establish persistence throughout the retailer’s network.

4

Search

The attackers identify valuable files to encrypt (e.g., customer PII, shipping logistics).

5

Encryption/Exfiltration

Attackers encrypt the retailer’s valuable files and may also keep a copy of the data.

6

Demand

Payment demands are made by the attacker in order to provide the decryption key or prevent the release of stolen data.

Ransomware Hex | Risks | Attack Anatomy | Protection | SageNet Effect | MNSP

Protecting Your Data from Illicit Incantations

To stymie the harmful consequences of ransomware, retailers can craft a protective shield to prevent attacks. Below are the steps you can follow to protect against ransomware:

1) Establish and enforce robust security and protection policies
2) Build and maintain a consistent and secure network across all locations (including affiliated suppliers)
3) Fortify access control and management
4) Deploy an event visibility and monitoring system and perform constant analysis
5) Design and implement continuous cybersecurity education and training programs for staff

> “*We work with a wide range of both small and large independent grocers, but they all have similar technology needs. With SageNet’s help, we meshed together a best-of-breed technology solution that helps their operations run efficiently, decreases costs, and increases capabilities.*”

RUSS GORMAN • Senior Project Lead • Bozzuto’s Inc., a leading grocery wholesaler

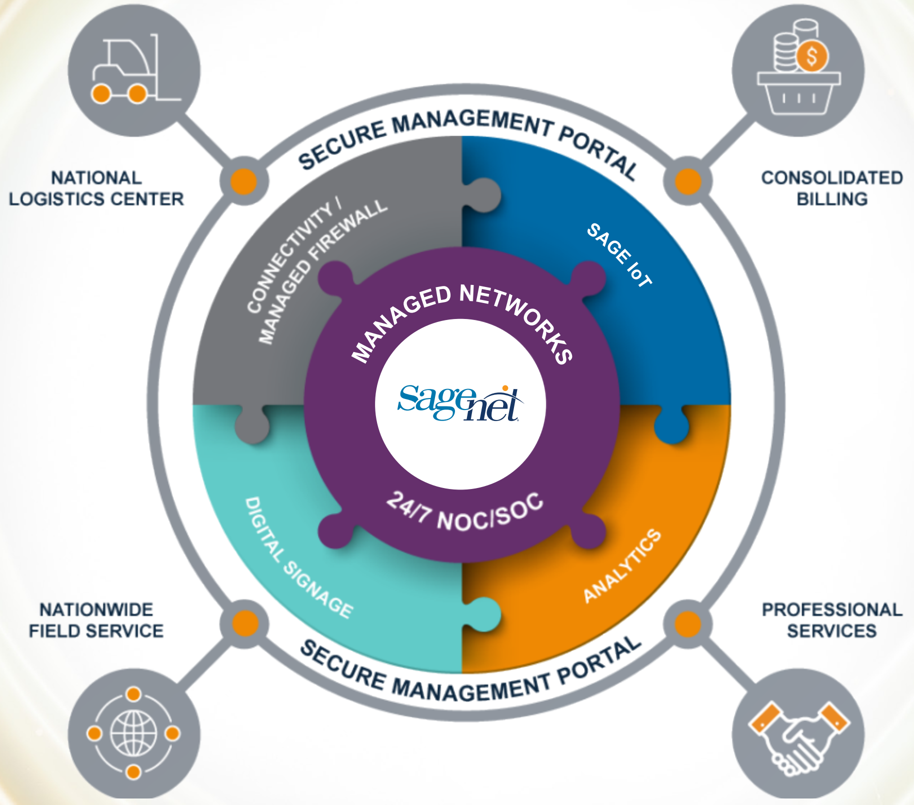
Ransomware Hex | Risks | Attack Anatomy | **Protection** | SageNet Effect | MNSP

SageNet: Demystify and Defeat Ransomware

To correctly and economically erect ransomware protection shields at scale, retailers need a seasoned network and security managed services provider. With more than 30 years of experience supporting some of America's leading retailers, SageNet has the technology, expertise, and support to build and secure modern networks, cloaking retailers in powerful ransomware protection.

From design to operations, SageNet delivers unparalleled managed networking services to retailers for store one to store 1,000 and beyond, protecting the entire supply chain and distribution network. Serving some of the top retailers across the country with over 15,000 locations, SageNet's team of certified network engineers, digital experience leaders, and cybersecurity experts adeptly safeguards retailers' business and customer data from ransomware.

SageNet SageSECURE offers a PCI-compliant, comprehensive managed services approach that follows a real-world proven way to connect, manage, and protect process. The SageSECURE platform delivers rapidly deployable, effective, and affordable connectivity, security, and digital signage solutions engineered specifically to protect the multi-site retailer from ransomware and empower the launching of next-gen stores, applications, and services.



Ransomware Hex | Risks | Attack Anatomy | Protection | SageNet Effect | MNSP

SageNet and Fortinet: Power to Thwart Ransomware

SageNet builds its digital ransomware protection shields with the most comprehensive and effective security solutions on the market. SageNet's managed network services are bolstered by a long-standing, extensive partnership with industry leader Fortinet. Producing the world's most deployed network security solutions, Fortinet delivers AI-based security, performance, and actionable threat intelligence to thousands of customers around the globe, including leading retailers.

Wielding the power of Fortinet to thwart ransomware, SageNet keeps retail data in safe hands, as every SageNet-optimized network is backed by three US-based 24/7 NOCs, and a state-of-the-art, nationwide service and support organization. By choosing SageNet, retailers gain peace of mind that comes from having a single point of contact for everything from implementation and management to security, billing, and support.

Set a Safe Environment with SageCONNECT™

SageCONNECT by SageNet enables the safe and high-performance networks that retailers need to win their customers' mind and wallet share. Using Fortinet FortiGate Next Generation Firewalls (NGFW) to thwart ransomware and other cyber threats to increasingly complex modern networks, many of the industry's leading retailers count on SageCONNECT for reliable, secure, and affordable connectivity.

SageCONNECT ensures continuous connectivity that produces exceptional customer experiences and revenue generation. SageNet Wi-Fi enables retailers to display unique branding for customer engagement, and auto-back-up services such as 5G coverage ensures locations can continue selling when primary connectivity fails. Plus, SageNet satellite services provide emergency communications and disaster recovery to enable business continuity.

sageCONNECT™

The Ultimate Ransomware Defense for Retailers

To cast the widest range for an invisible, yet powerful ransomware protection barrier, multi-site retailers can adeptly prioritize and route their networking traffic with SD-WAN architecture. SageCONNECT is SageNet's Fortinet-based SD-WAN solution that delivers the network flexibility, efficiency, availability, and security that multi-site retailers require, along with 24/7/365 monitoring and support.

By leveraging the built-in SD-WAN capabilities provided by FortiGate NGFWs, SageCONNECT combines robust, high-availability networking with enterprise-class security to stop cyber threats. By offering automated path intelligence, tunnel bandwidth aggregation, and best-of-breed NGFW and unified threat management (UTM), SageCONNECT enables retailers to scale their operations with the confidence that their data, applications, and critical resources are well protected from ransomware.

Ransomware Hex | Risks | Attack Anatomy | Protection | SageNet Effect | MNSP

sageSECURE™

Enhance the Potency with SageSECURE™

SageNet's security team helps retailers increase visibility, detection, and response; achieve PCI 4.0 compliance to ensure continuous operations, protect critical data, and conduct employee training for ransomware prevention.

sageIoT™

Ensure a Receptive Audience with SageIoT™

Leverage predictive analytics to better understand the retail audience with an IoT visibility platform that monitors activities and identifies issues, so SageNet can respond to optimize network performance with precision.

sageVIEW™

Impact the Entire Crowd with SageVIEW™

Display safe and secure digital signage-as-a-service (DSaaS) to increase revenue, influence purchase decisions, and improve operational performance and efficiencies. Plus, SageNet Experience Labs will help design the most effective content for engagement and scale.

SageNet Managed Network Services

Entrust SageNet's industry-leading managed services, extensive partnerships, and networking and cybersecurity expertise to craft the ultimate ransomware protection shield for your retail operation. With SageNet as your managed network services provider, you can improve operational performance, enhance customer experiences, and grow revenue, all while keeping your employees and customers safe from ransomware and other cyber threats.

Contact SageNet today to counteract the ransomware hex or email us for more information.

SOURCES:

1) Sophos, The State of Ransomware in Retail 2023, July 2023.
2) Ibid.
3) Cybereason, Ransomware: The True Cost to Business 2022, June 2022.
4) The Guardian, JD Sports hit by cyber-attack that leaked 10m customers' data, January 2023.
5) Fortinet, 'Tis the Season for Cyberattacks. Retailers: Here's How to Protect Your Brand, November 2022.
6) Cybersecurity Drive, NCR in recovery as ransomware disrupts widely used point-of-sale system, April 2023.