Peoplebank

ZURICH
Resilience Solutions

GUIDE:
The Rise of Ransomware and How to Fight Back

What is Ransomware

Ransomware is a type of malicious software (malware) that encrypts a victim's files or systems, rendering them inaccessible until a ransom is paid.

Key Characteristics

Ransomware is a type of malicious software designed to block access to a computer system or encrypt its data until a sum of money, or ransom, is paid. Attackers typically demand payment in cryptocurrency to maintain anonymity and often threaten to permanently delete or publicly leak the stolen data if their demands are not met.

Common Targets

- Enterprises
- Healthcare institutions
- Government agencies
- Critical infrastructure

Ransomware Anatomy

Recognition & Targeting

Attackers research and select a target, identifying vulnerabilities to exploit.

Infiltration

Hackers breach the network, through phishing email or stolen password etc.

Command & Control

The attacker establishes a remote, hidden connection to the compromised system.

Lateral Movement

The hacker spreads through the network to access more critical systems and data.

Exploit

The ransomware is deployed to encrypt files and/or steal sensitive data.

Extortion

The attacker demands payment to restore access or prevent data leaks.

Worldwide Ransomware Attacks (2024)

Year	2022	2023	2024
No. of Attacks	2,593	4591 (77% ↑)	5289 (15% ↑)

Payment to ransomware attackers, data theft and extortion gangs

2023	2024
$1.25B	$814M

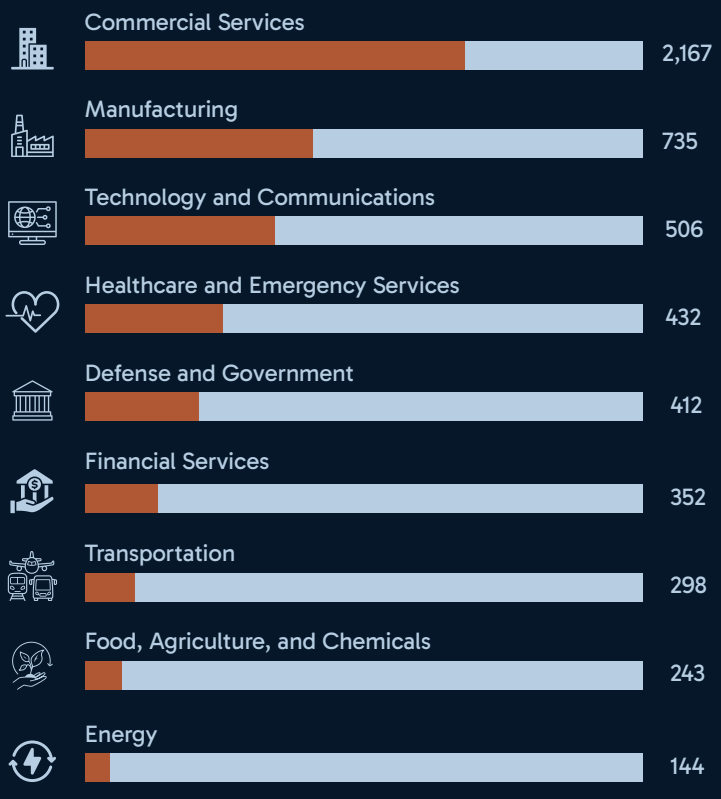
Total volume of ransom payments YoY

35% ↓

Despite the decrease in ransom payments, the threat is evolving, not receding.

Cybercriminals are adapting with AI-powered attacks, more sophisticated extortion tactics, and targeting critical infrastructure. Proactive defense is now more critical than ever.

Total ransomware attacks worldwide by industry (2024)



Ransomware as a Service (RaaS)

A massive and unsuspected attack surface

The Affiliate

The one who want to attack and make money

- Identifies an opportunity
- Contact a broker and/or trader
- Receives a share of earnings

The Broker

Exploits a vulnerability & breach the corporate network

- Recovers user accounts
- Uses bots
- Launch the Attack (Exploit)
- Maintain remote access

The Operator

Develops and maintains malicious tools and services

- Creation of the ransomware
- Site to collect stolen data
- Communication with victims
- Payment processing and laundering

The Victim

The one who suffers the damage and pays the ransom

CASE STUDY: The M&S Ransomware Breach

Feb 2025

Attackers gain access to the M&S network using stolen credentials from an employee of Tata Consultancy Services (TCS), a key IT partner of M&S.

They stole the **NTDS.dit file**—the network's "master key" containing all passwords and permissions.

Apr 2025

Ransomware was deployed via **DragonForce**, a cybercrime-as-a-service platform.

Attackers sent a ransom demand email to M&S's CEO, gloating about the breach and demanding payment.

What is NTDS.dit?

NTDS.dit acts as the address book and rulebook for a company's computer network. It stores usernames, passwords, group memberships, permissions, etc. If someone gets access to this file, they could potentially access everything in the network. That's why it's heavily protected and only accessible by system administrators.

Impact

System Affected

Online payments, click-and-collect, contactless store payments.

Data Breach:

Customer names, addresses, emails, DOBs, order history.

Threat Actors

DragonForce

A ransomware-as-a-service (RaaS) operation that allows cybercriminals to deploy ransomware under a white-label model.

Scattered Spider

A cybercrime group targeting major retail and financial enterprises through social engineering (SIM swapping, MFA fatigue attacks etc.), credential harvesting, and Active Directory exploitation.

Lessons Learned

1

Incident Response

M&S responded quickly, but communication with customers needs improvement during incidents.

2

Third-Party Risk

Third-party service providers introduce vulnerabilities that can be exploited. Companies must manage these risks.

3

Data Minimization

Limiting stored data reduces the impact of breaches, protecting sensitive information.

Combating Ransomware

Technical Controls

MFA Enhancement
Upgrading authentication methods with MFA to resist phishing attacks

Access Control
Enforcing least privilege principles and regular reviews

Zero Trust
Verifying all users and devices rigorously

EDR Deployment
Implementing real-time threat detection and repsonse

Network Segmentation
Isolating critical systems to prevent lateral movement

Secure Remote Access
Monitoring and securing remote access tools

Reconnaissance Reduction
Use WAFs, disable directory listings to limit publicly available information

Operational Controls

Third-Party Risk Management
Regular security assessments and audits of vendors to ensure compliance and security.

Incident Response Drills
Simulating modern attack scenarios to test and refine incident response playbooks.

Data Encryption and Backup
Encrypting sensitive data and ensuring backups are isolated and protected.

Telecom Coordination
Adding friction to SIM swap processes to protect high-risk users.

Human Factors

Security Awareness Training
Educate employees on phishing, credential theft, social engineering, and how to report suspicious activity.

Helpdesk Security Protocols
Train support teams to verify identities robustly and resist social engineering attempts.

Communication Preparedness
Develop and pre-approve internal and external messaging templates for use during incidents.

*All content and insights are provided by **Zurich Resilience Solutions**

Ruiwen Wan

Cyber Risk Team Lead, Hong Kong

With more than 8 years of experience in the three lines of defense, Ruiwen's expertise covers a range of areas in cyber resilience, especially in financial industry.

Kennedy Kan

Senior Cyber Risk Engineer, Asia

Kennedy brings over 8 years of experience in information security and IT risk management, developing a strong track record of success in enhancing the cyber resilience.