

The Industrialized 「**RANSOMWARE**」

— Anyone can become an attacker.

01

The Rise of RaaS¹

¹RaaS: Ransomware as a Service

Ransomware is **no longer a one-off attack.**

Today, it follows a repeating cycle:

1



Exfiltration

2



Negotiation

3



Leak

4



Re-negotiation

▶ At the core of this evolving threat is RaaS.



02

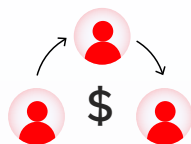
How **RaaS** Works

RaaS divides the attack process into **distinct roles**.



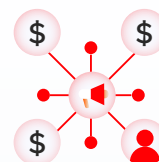
Operator

Develops ransomware and maintains infrastructure



Access Broker

Obtains and sells compromised credentials or exploits



Affiliate

Purchases access and tools and executes attacks



Technical skills are no longer a barrier.



03

Recent 「RANSOMWARE」 Incidents



Europe – Major Airports Paralyzed by Ransomware

- Widespread flight delays and cancellations at Brussels, Heathrow, and others



Japan – Asahi Group Ransomware Attack

- Production and distribution systems disrupted
- 27GB of data exfiltrated



South Korea – Financial Institution Ransomware Attack

- Services suspended for 4 days
- 24 out of 79 claims compensated (₩11.9M / ~\$9K USD)





04

Integrated Security Strategy

- 1 Employee training and awareness**
Conduct regular simulations to improve response readiness
- 2 Enhanced backup and recovery system**
Maintain offline backups and rapid recovery systems
- 3 Prevention of internal threat spread**
Implement least privilege access & monitor for anomalies
- 4 Early attack path detection and blocking**
Monitor vulnerabilities and apply patches



05

VNETWORK's EG-Platform

The only email solution that achieves 100% ITU compliance and is recognized by top international authorities.



Real-time threat analysis from email receipt



Zero-trust multi-layered scanning

(URLs, attachments, QR codes, etc.)



AI-powered behavior analysis



Synchronized modules for comprehensive security

Email Gateway Platform

Comprehensive Email Security powered by AI/ Machine learning

Register now →

Summary of Diagnosis

[Company Name]'s email security c from [dd-mm-yyyy] to [dd-mm-yyyy] of total [n] total emails, [n] caution dangerous emails were detected. S potentially harm your computer ar losses to your organization throug personal data breaches. Therefore advised. We recommend updating security solution, or if you are not one, we strongly encourage impler solution that can block such emails

Overall Results of Email D

Cautionary Email	First-level Filter
Dangerous Email	Business/Prom
	Malware (Malic
	Malicious URL
	Ransomware
	Conditional B
Tampered Email	Forged Header
	Sender Locatio
	Look-alike Don

Inbound Emails by Vulner

Information Leakage	[n]
---------------------	-----

Top 5 Users Requiring Cau

[Company Name]

Result of Final Diagnosis

Based on the results detected during the diagnostic period, the final checklist and recommended guidelines are provided.

Guidance

Classification	Case(s)	Checklist
Dangerous Email	Business/Promotional Spam	[n] Please check the email security solution to ensure that both busi and promotional mails are blocked. If there are any emails that h not been blocked, it is recommended to update the email securit solution.
	Malware	[n] To proactively block dangerous emails classified as malicious activitie is recommended to utilize an email security solution with the capabil analyze all behaviors of email.
	Malicious URL	[n] To proactively block malicious URLs, it is recommended to set up option to receive emails only from authenticated senders when dealing with a significant volume of emails containing links.
	Ransomware	[n] By allowing only emails that meet specific criteria, such as a fixed IP or other specified conditions, you can proactively block emails classified ransomware.
Tampered Email	Forged Header	[n] We recommend implementing an email security policy that priori blocking emails where the actual sender's email address differs f the one visible to the recipient.
	Sender Location Change	[n] We recommend offering a separate notification feature for email originating from high-risk countries to provide users with an aler take necessary precautions as a default response.
	Look-alike Domain	[n] We recommend using an encrypted secure email service to enable immediate differentiation between regular emails and emails sent by hackers.

Recommendations

We recommend using an email security solution equipped with the following features:

- Separate notification for emails with altered senders,
- Receiving emails only from fixed IP addresses,
- Separate notification for emails with sender addresses different from previous email history or other pattern